Regular Paper

IoTPOT: A Novel Honeypot for Revealing Current IoT Threats

Yin Minn Pa Pa^{1,a)} Shogo Suzuki¹ Katsunari Yoshioka¹ Tsutomu Matsumoto¹ Takahiro Kasama² Christian Rossow³

Received: June 30, 2015, Accepted: January 12, 2016

Abstract: We analyze the increasing threats against IoT devices. We show that Telnet-based attacks that target IoT devices have rocketed since 2014. Based on this observation, we propose an IoT honeypot and sandbox, which attracts and analyzes Telnet-based attacks against various IoT devices running on different CPU architectures such as ARM, MIPS, and PPC. By analyzing the observation results of our honeypot and captured malware samples, we show that there are currently at least 5 distinct DDoS malware families targeting Telnet-enabled IoT devices and one of the families has quickly evolved to target more devices with as many as 9 different CPU architectures.

Keywords: IoT, Honeypot

1. Introduction

Since years, it is known that many Internet of Things (IoT) devices are vulnerable to simple intrusion attempts, for example, using weak or even default passwords [1]. In 2012, Carna botnet [2] revealed that there were more than 1.2 million open devices that allowed logins with empty or default credentials. In January 2014, an Internet-connected fridge was discovered as a part of a botnet sending over 750,000 spam e-mails [3]. In December 2014, online DDoS services (i.e. booters) knocked down Sony and Microsoft's gaming networks, presumably powered by thousands of compromised IoT devices such as home routers [4]. From an attacker's point of view, IoT devices are attractive playgrounds, as-as opposed to PCs-they are 24/7 online, have no antivirus installed, and weak login passwords give attackers an easy access to powerful shells (such as BusyBox [5]). Seeing these trends, we believe that IoT devices are an important new area of security research.

In this paper, we investigate the threat of IoT device compromises in the masses. We first analyze Telnet-based scans in darknet, revealing that attacks on Telnet have rocketed since 2014. Moreover, by grabbing Telnet banners and web contents of the attackers, we show that the majority of attacks indeed stem from IoT devices.

Motivated by this, we propose IoTPOT, a novel honeypot to emulate Telnet services of various IoT devices to analyze ongoing attacks in depth. IoTPOT consists of a frontend low-interaction responder cooperating with backend high-interaction virtual environments called IoTBOX. IoTBOX operates various virtual en-

¹ Yokohama National University, Yokohama, Kanagawa 240–8501, Japan

^{a)} yinminpapa@gmail.com

vironments commonly used by embedded systems for different CPU architectures. During 81 days of operation, we observed 481,521 download attempts of malware binaries from 79,935 visiting IP addresses. We also confirm that none of these binaries could have been captured by existing honeypots that handle the Telnet protocol such as honeyd and Telnet password honeypot because they are not able to handle different incoming commands sent by the attackers.

We manually downloaded 106 distinct malware samples and found out that they run on 11 different CPU architectures. Among 106 collected samples, 88 samples were new to the database of VirusTotal [6] (as of 2015/06/26) showing a gap of capturing utilities for this type of threat. Out of 18 samples in VirusTotal, 2 of them were not detected by any of the 57 antivirus software of VirusTotal (as of 2015/06/26).

In order to analyze these captured malware binaries, we propose IoTBOX, the first malware analysis environment for IoT devices. IoTBOX supports 8 CPU architectures, spanning MIPS, ARM, and PPC. The sandbox analysis of 25 samples by IoTBOX revealed that the samples are used to perform 11 different types of DDoS attacks, port 23 scans and scans on UDP (port 123, 3143) and TCP (port 80, 8080, 5916).

Finally, combining the observations results of IoTPOT with the sandbox analysis by IoTBOX, we confirm that i) there are at least five distinct malware families spreading via Telnet, ii) their common behavior is performing DDoS and the further propagation over Telnet, iii) some families evolve quickly, updating frequently and shipping binaries for a variety of CPU architectures, even in the limited observation period of 81 days.

Following is the summary of our contributions:

1) We point out a huge increase of Telnet-based attacks and the

 ² National Institute of Information and Communications Technology, Koganei, Tokyo 184–8795, Japan
 ³ Dela Huissia (2020 participation)

 ³ Saarland University, 66123 Saarbrücken, Germany
 ^{a)} vinminpapa@gmail.com

Part of the results of this paper will be presented at the 9th USENIX Workshop on Offensive Technologies (WOOT'15).

involvement of IoT devices.

- 2) To analyze the scope and variety of the attacks, we propose a novel honeypot called IoTPOT, which mimics IoT devices and captures Telnet-based intrusions.
- 3) We further analyze the threats and propose IoTBOX, which enables us to run the captured malware on 8 different CPU architectures.
- 4) We reveal that there are at least five DDoS malware families targeting IoT devices.
- 5) We analyze the architectures of IoT botnets and point out that there are at least 8 different types of botnet architectures including the worm type botnet.

The rest of the paper is organized as follows: Section 2 explains our preliminary investigations on Telnet-based attacks. Section 3 describes IoTPOT and Section 4 IoTBOX. In Section 5, we describe the overview of ongoing attacks revealed by our analysis. In Section 6, related works are presented. Finally, in Section 7 the conclusion and future works are explained.

2. Investigation on Telnet-based Attacks

Until now, there are only anecdotal reports on Telnet-based compromises. In this section, we investigate how the situation of Telnet-based compromises has changed. To this end, we analyze a darknet of NICTER [7], Japan's darknet monitoring system that monitors over 209,000 IP addresses presently.

Figure 1 shows the traffic on 23/TCP since 2005, both in terms of packets and source IP addresses per day (averaged over all IP addresses in the darknet). The data shows a recent increase of scans for Telnet. According to the previous study [8], the large peak in the end of 2012 is caused by the activities of the Carna botnet, created by an anonymous hacker for Internet Census by compromising a large number of IoT devices such as routers [2]. Since 2014, even after the deactivation of the Carna botnet, both the number of packets on 23/TCP and their senders have rapidly increased and dominated the darknet – observing more than 209,497 average scanning sources per day, which is 52.5% of all sources, in the darknet in the first week of March 2015.

We used p0f for passive OS fingerprinting [9] and determined that among the scanning 29,844 hosts (sampled from 148 darknet IP, 2015/03/05 to 2015/03/10), 91% of them runs Linux. We also connected back to these hosts on 23/TCP and 80/TCP, collected Telnet banners and web contents if any, and manually categorized them by device types. For example, if there is a telling keyword such as "DVR" in HTTP title, we categorize this device as Digital Video Recorder (DVR). If not, we search on the Internet using the HTTP title as keyword and carefully categorize devices by reading available manuals. We also group device models of a particular device type by different HTTP titles. For example, HTTP titles such as "NetDVrV1" and "NetDvrV3" will be counted as two device models of DVR device type. With this way, we found more than 34 different types of IoT devices including 19 different models of the DVR, 16 models of IP Camera, 45 models of wireless routers. Moreover, devices such as a metrological satellite, heat pumps, a parking management system, a fire alarm system, solid state recorders and a TV have scanned our darknet on 23/TCP.

© 2016 Information Processing Society of Japan



Fig. 1 Packets and hosts on 23/TCP per day per darknet IP.

Table 1Scanning hosts and device models.

Devrice Turne	Host	Device	
Device Type	Count	Model Count	
DVR	1,509	19	
IP Camera	523	16	
Wireless Router	118	45	
Customer Premises Equipment	65	1	
Industrial Video Server	22	1	
TV Receiver	19	2	
Heat Pump	10	1	
Environment Monitoring Unit			
(EMU) System	9	1	
Digital Video Scalar	5	2	
Router	4	3	

Table 1 shows top ten attacking hosts and device models of inferred device types. These results show that various IoT devices are already involved in the ongoing attacks.

3. IoT Honeypot (IoTPOT)

Our preliminary investigation on Telnet-based attacks implies that there are a number of IoT devices being compromised and misused to search and attack other IoT devices. In order to study these attacks in depth, we propose IoTPOT, a novel honeypot that emulates interactions of the Telnet protocol and a variety of IoT devices.

3.1 Telnet Protocol

Before explaining IoTPOT, we briefly revisit the Telnet protocol [10]. **Figure 2** illustrates the interactions between client and the server on Telnet. After the TCP 3-way handshake, the client and the server can exchange Telnet options. Either the Telnet server or the client can initiate a request such as "Do Echo", a request for echo back and "Do NAWs" a request to Negotiate About Window size (NAWs). After exchanging options, the server sends a welcome message to the client, immediately followed by the login prompt. For example, "BCM96318 Broadband Router" as the welcome message and "Login:" as the login prompt. In this paper, we call the above initial part of interactions **banner inter-**



actions. Then, the client sends a pair of username/password to log in to the server. We call this part **authentication**. Finally, if the credentials are valid, the client logs in and instructs the server using various shell commands. We call this part **command inter-actions**.

3.2 IoTPOT Design

The Telnet protocol already highlights a few challenges for our honeypot design. First, we need to support options that the attacking clients choose to use. Second, we aim to provide a realistic welcome message and login prompt, to deal with situations where an attacker specializes in compromising certain devices only. Third, we want to allow for logins, while we also want to observe characteristics in the authentication interactions (e.g., sequences of usernames/passwords). Finally, independent from the Telnet protocol, our honeypot should support multiple CPU architectures to capture malware across devices. Our honeypot is designed to support these features.

In order to emulate different devices, we collected these banners from the Internet by performing Telnet scans with the masscan tool [11]. From all collected banners, we prioritized banners of hosts that have accessed our honeypot. Considering a selfspreading nature of these attacks, these attacking hosts can also be considered as already compromised victims, which should be emulated by our honeypot.

In the next step, during the authentication, IoTPOT supports various tactics. For example, it can be configured to reject any authentication credentials to observe login attempts, to allow immediate authentication regardless of the login, to accept only certain credentials, or reject the first attempts and eventually accept a login. Finally, during a command interaction, the frontend responder of IoTPOT replies known commands from attackers and unknown commands are redirected to backend embedded Linux OSs of different CPU architectures. As each IoT device runs on a different CPU architectures to handle the interactions of various devices.



Fig. 3 Overview of IoTPOT.

3.3 IoTPOT Implementation

Figure 3 is the overview of IoTPOT. The heart of IoTPOT is *Frontend Responder*, which acts as different IoT devices by handling incoming TCP connection requests, banner interactions, authentication, and command interactions with a set of device profiles.

A device profile consists of a banner profile, an authentication profile, and a command interaction profile. Banner profiles determine the responses of the honeypot for banner interactions, namely Telnet options, a welcome message, and a login prompt. Authentication profiles determine how to respond to incoming authentication challenges. The command interaction profile determines the responses to incoming commands, consisting of a set of commands and their corresponding responses.

When an incoming command is not known yet, *Frontend Responder* establishes a Telnet connection with a backend IoTBOX and forwards the command to it. IoTBOX is a set of sandbox environments that run Linux OS for embedded devices with different CPU architectures. When an incoming command does not match with any commands in the command interaction profile, thus unknown to *Frontend Responder*, it establishes a Telnet connection with a backend IoTBOX and forwards the command to it. IoTBOX is a set of sandbox environments that run Linux OS for embedded devices with different CPU architectures. Namely, if an unknown command from an attacker comes to *Frontend Responder* with the device profile of some device X assigned, we forward the unknown commands to the sandbox running the CPU architecture of the device X.

As described later, banner profiles are collected by banner grabbing of IoT devices visiting to IoTPOT and their respective CPU architectures are manually chosen by carefully reading a device manual and the maker's website. If we cannot find explicit CPU information of a particular IoT device, we refer to the list of applications for each CPU architecture [12], [13], [14], [15], [16].

Frontend Responder forwards a response from IoTBOX to the client. Note that the incoming commands forwarded to IoTBOX may cause malware infections or a system alteration. Therefore, we reset the OS image occasionally. Moreover, IoTBOX in IoT-POT is used as a high interaction system to reply to commands unknown to the *Frontend Responder* as a component of IoTPOT.

We also use IoTBOX independently for analyzing captured malware binaries. The detailed explanation of IoTBOX is in Section 4.

The *Profiler* parses the interaction between *Frontend Responder* and IoTBOX, extracts the incoming command and the corresponding response, and updates the command interaction profile so that *Frontend Responder* can further handle the same command without interacting with IoTBOX. Another important function of *Profiler* is the collection of banners from devices on the Internet. The *Profiler* operates in two banner grabbing modes: active scan mode and visitor scan mode. In active scan mode, *Profiler* scans different networks to collect banners from various devices. In the visitor scan mode, it connects back to hosts who visit our honeypot and grabs the banners.

The *Downloader* component examines the interactions for download triggers of remote files, such as malware binaries. In particular, we download from all URLs we observed via commands such as *wget*, *ftp*, and *tftp*.

Finally, network communications between *Frontend Responder* and IoTBOX are controlled by *Manager* implemented by iptables [17].

3.4 Observation Results

IoTPOT Setup: We operated IoTPOT in two different periods: Trial operation period and stable operation period. In the trial operation period from 2014/11/07 to 2015/03/31, we had tried different configurations, device profiles, and assignment of IP addresses in a ad-hoc manner trying to understand the attackers' behavior and discussing the proper setting of the honeypots. In the stable operation period from 2015/04/01 to 2015/06/20, we deployed IoTPOT on 87 IP addresses, used 29 banner profiles assigning each to three IP addresses. We set authentication profiles to accept any challenges and prepared a single command interaction profile, manually created from one of the most widely exploited DVR brands [18]. The backend IoTBOX contained an embedded Linux OSs of Debian [19] and OpenWrt [20] on 8 different CPU architectures emulated by QEMU [21]. Downloader was not fully implemented so we manually downloaded and collected malware binaries.

Summary of Observations: During 81 days of the stable operation, 180,581 hosts visited IoTPOT. Among them, 130,314 successfully logged in and 79,935 attempted to download external malware binary files. We observed 481,521 download attempts in total. We manually downloaded 106 malware binaries of 11 CPU architectures. Among 106 collected samples, 88 samples were new to the database of VirusTotal (as of 2015/06/26). Out of 18 samples that were in VirusTotal, 2 of them were not detected by any of the 57 antivirus software of VirusTotal (as of 2015/06/26). General Flow of Telnet Attacks: We observed three typical steps of compromise: 1) The first stage of attack is intrusion, in which attackers attempt to login to our honeypot. The intrusion normally starts from scanning the targets and then dictionarybased authentication challenges. 2) The second stage after the successful intrusion is infection, in which attackers send a series of commands over Telnet to check and customize the environment, download and execute the external binaries. 3) The third

Table 2 Major log in patterns observed by IoTPOT.

Pattern Name	Challenge Order	Username/Pass	
		root/root root/admin	
		root/1234	
	Fixed Order	root/12345	
Enad Onder		root/123456	
Fixed Order		root/1111	
1		root/password	
		root/dreambox	
		root/vizxv	
		root/system	
		admin/admin	
		root/root	
		root/admin	
		root/12345	
Random Order	Parada and Onder	root/123456	
1	Random Order	admin/root	
		admin/admin	
		support/support	
		admin/admin	
		admin/362729	
		admin/m4f6h3	
Fixed Order	Fixed Order	admin/n3wporra	
Fixed Ofder	Fixed Order	admin/263297	
4		admin/fdpm0r	
		admin/1234	
		root/1234	
		root/xc3511	
Pandam Order		root/123456	
Random Order	Random Order	root/12345	
2		root/root	
		guest/guest	
		guest/12345	
		admin/	
		root/root	
		root/admin	
Fixed Order	Fixed Order	root/	
3	Fixed Order	root/1234	
		root/123456	
		root/1111	
		root/password	
		root/dreambox	
		rost/vizxv	
		root/root	
		root/toor	
		root/admin	
Random Order	Random Order	root/user	
3	Randoll Order	root/guest	
		root/login	
		root/changeme	

stage after the infection is monetization, in which executed binaries are controlled by the attackers through C&C to conduct the intended malicious activities such as DDoS attacks and spreading of malware. Note that we intend to observe the intrusion and the infection by IoTPOT and after malware binaries are captured by IoTPOT, we conduct a sandbox analysis using IoTBOX. Thus in this experiment, IoTBOX is utilized in two ways, as a backend component of IoTPOT and as an independent sandbox analysis environment for analyzing the obtained binaries. The following subsections highlight some points noticed for each attack stage. The overall relationships among attacks observed at different stages are summarized in Section 5.1.

3.4.1 Stage 1: Intrusion

We recognize two major intrusion behaviors: login attempts with a fixed or a random order of credentials. Table 2 shows the major login patterns observed by IoTPOT. Fixed challenge order, "Fixed Order," in Table 2 means attackers try to login to IoTPOT with a sequence of id and password pairs in a fixed order. For example, in the case of a pattern name, "Fixed Order 1," the attacker's challenge always starts from "root/root" as user id and password to login to IoTPOT. Then, the pairs, "root/admin," "root/123," "root/12345" come in a fixed order of sequence till it reaches to "admin/admin." Thus, for the fixed login sequences, we can reasonably infer that these challenges are from malware sharing the same implementation of dictionary attacks. "Fixed order 2" in Table 2 is quite a long list, thus, we show only top sequences. Random challenge order means attackers try to login to IoTPOT with a sequence of id and password pairs in a random order. Thus, in case of "Random Order 1," it is not always true that "root/admin" will come after "root/root."

3.4.2 Stage 2: Infection

After successfully logged in to honeypot, attackers check and customize the environment to prepare the download of a malware binary by sending a series of commands over Telnet. **Table 3** **Table 3** Patterns of command sequence observed by IoTPOT.

Pattern Name	Pattern of Command Sequence
	 Check type of victim shell with command "sh" Check error reply of victim by running non-existing command such as ZORRO. Check whether wget command is usable or not. Check whether behave held as the provide state of the providest s
ZORRO I	 Check whether busybox shell can be used or not by echoing ZORRO. Remove various command and files under /usr/bin/, /bin, var/run/, / dev. Copy /bin/sh to random file name Append series of binaries to random file name of stop 6 and males.
	 Append series of binaries to random inc mane of step 5 and mare attacker's own shell Using attacker's own shell, download binary. IP Address and port number of malware download server can be seen in the command. Run binary
	 Check type of victim shell with command "sh" Check error reply of victim by running non-existing command such as ZORRO. Check whether wget command is usable or not.
ZORRO 2	 Check whether busybox shell can be used or not by echoing ZORRO. Remove various command and files under /usr/bin, /bin, var/run, / dev. Copy /bin/sh to random file name
	7. Append series of binaries to random file name of step 6 and make attacker's own shell 8. Using attacker's own shell, download binary . IP Address and port number of malware download server cannot be seen in the command because it is hard coded in the attacker's own shell.
	 Check type of victim shell with command "sh" Check error reply of victim by running non-existing command such as ZORRO. Check whether weet command is usable or not.
ZORRO 3	 Check whether busybox shell can be used or not by echoing ZORRO. Remove all under /var/run, /dev, /tmp, /var/tmp Copy /bin/sh to random file name Append series of binaries to random file name of step 6 and make attacker's own shell Using attacker's own shell, download binary. IP Address of malware download server can be seen in the command and nort number
	cannot be seen in the command 9. Run binary 1. Check error reply of victim by running non-existing command such as "enable" or "shell". 2. Check type of victim shell with command "sh"
ZORRO 4	 Remove all under /var/run, /dev, /tmp, /var/tmp Copy /bin/sh to random file name Append series of binaries to random file name of step 4 and make attacker's own shell, download binary. IP Address of malware download server can be seen in the command and port number cannot be seen in the command Run binary.
GAYFGT 1	 Check whether shell can be used or not by echoing "gayfgt" Download shell script. Using downloaded shell script, kill previously running malicious process, download malware binaries of different CPU architectures and block 23/TCP in order to prevent other infection. Run all downloaded malware binaries.
GAYFGT 2	 Check type of victim shell with command "sh" Download shell script. Using downloaded shell script, download malware binaries of different CPU architectures. Run all downloaded malware binaries. Make sure shell is Busybox by echoing binary that will encode into "gavfgt" only in Busybox shell.
*.sh	 Download shell script using wget command. Using downloaded shell script, download malware binaries of different CPU architectures. Run all downloaded malware binaries.
nttpd 1	 Check whether shell can be used or not by echoing "welcome" Download binary to /tmp directory. Run Binary.
nttpd 2	 Check whether shell can be used or not by echoing "welcome" Remove file names, .nttpd and .drop, from /tmp directory. Make new file names, .nttpd and .drop. Append binaries of malware through Telnet commands to .drop file. S. Run Binary
KOS	 Check whether shell can be used or not by echoing "S? K_O_S_T_Y_P_E" List /proc/self/exe Check all running process Download malware binary using tftp to /mnt folder Run Malware Check CPU information

summarizes the 10 major patterns of command sequences observed by IoTPOT. Note that some of the patterns were observed only in the trial operation period for parameter tuning and we do not have credible counts of these patterns. We believe most
 Table 4
 Clustering results of collected samples by characteristic strings in the binaries.

Family Name	Common Strings in Binaries
Bin 1 - Bin 9	YESHELLO
	killattk
	SCANNER ON OFF
	bin.sh
Bin 10 to Bin 41	bin2.sh
	bin3.sh
	echo -e '\x67\x61\x79\x66\x67\x74'
	sh -c "cd /tmp ; rm -f .nttpd ; wget -O .nttpd
Bin 42	http://%d.%d.%d.%d:%d ; chmod +x
	.nttpd ; ./.nttpd"
	0916.davinci
Bin 43	0923.davinci
	0923.8196

infection activities are automated as exactly the same pattern of commands are repeatedly observed and also the intervals between the commands are very short.

We name each pattern by the characteristic string it contains. For example, the patterns named ZORRO 1, ZORRO 2 and ZORRO 3 all have the common string "ZORRO" in their command sequences. Moreover, we can see the attacker's common intension among them. Namely, all three patterns of ZORRO try to remove many existing commands and files under /usr/bin, /bin/, etc, and prepare a customized command for downloading an external malware binary file. With this setup, other intruders would have difficulty to abuse the system. A similar intension of attackers can be seen in the case of a pattern named GAYFGT. Although it does not alter the commands, instead it activates iptables [17] to drop incoming telnet connection requests. GAYFGT also has a functionality to kill other existing malicious processes. All these activities explained above come in a form of commands over Telnet except that GAYFGT downloads and executes shell script file to do it. Although there are diversities in attackers' behavior at the infection stage, they all have a common goal of downloading and executing malware binary file. One more common behaviors we found is checking whether the shell is usable properly or not by echoing a particular string in all families. If the appropriate reply for the echo command is not received, the attacker stops the attacks.

Comparison with honeyd: We confirmed that honeyd [22] cannot handle these commands in Table 3 and therefore cannot capture malware binaries observed by IoTPOT. Namely, honeyd failed to respond to the very first few commands such as "cat /bin/sh" in case of the ZORRO family and appropriate reply for the first echo command of GAYFGT, nttpd and KOS family and so the attacker stopped sending any further commands.

Clustering of binaries captured by IoTPOT: Within the first 39 days of operation of IoTPOT (From April 1, 2015 to May 9, 2015), the collected 43 samples are not obfuscated and relatively easy to cluster by checking whether these binaries contain certain characteristic strings or not. Namely, we classified the binaries based on the hardcoded human readable strings contained in the malware binaries such as strings for C&C commands, Linux commands and file names. We analyze the strings in binaries using the strings command of Linux. **Table 4** summarizes results of manual clustering of the collected samples based on the common

strings in the binaries.

Within the last 42 days of operation of IoTPOT (From May 10, 2015 to June 20, 2016), the number of captured malware increased more than double (Total 106 samples). Some of the binaries are obfuscated and so the approach to cluster the binaries using just strings command is then difficult. We need to find a better way to cluster these obfuscated binaries. This will be future works for us. Thus, for Bin 44 to Bin 106 of Appendix, samples we newly captured within the last 42 days, we cluster them into the same group if the command sequence from an attacker is similar to the previously categorized 43 samples.

3.4.3 Stage 3 Monetization

IoTPOT can only observe intrusion and infection stages explained in Section 3.4.1 and Section 3.4.2. Thus, in order to further reveal how attackers are trying to monetize the compromised devices, we analyze the malware binaries collected by IoTPOT using IoTBOX as an independent malware sandbox. We show the list of samples in the Appendix. The sandbox analysis results of some of the binaries are described in Section 4.

4. IoT Sandbox (IoTBOX)

IoTBOX is used not only as high interaction systems in IoT-POT but also as a stand-alone multi-architecture sandbox. The design of IoTBOX used for two purposes is the same and only routing policies are different for each purpose. So we discuss about IoTBOX design in general first and then explain consecutively how we define routing policies for IoTBOX in IoTPOT and IoTBOX as a stand-alone multi-architecture sandbox in Section 4.1.

4.1 IoTBOX Design

IoTBOX supports 8 different CPU architectures, namely as MIPS, MIPSEL, PPC, SPARC, ARM, MIPS64, sh4 and X86. The design of IoTBOX is shown in **Fig. 4**. To support different CPU architectures, we need a cross compilation environments. We thus choose to run respective platforms (OS) on an emulated CPU using QEMU [21], an open source processor emulator. Then, we use the respective OpenWrt platform to run on the emulated CPU environment. OpenWrt is a highly extensible GNU/Linux distribution for embedded devices of (typically



Fig. 4 Overview of IoTBOX

OS of wireless routers) [20]. To install OpenWrt, we use Open-Wrt Builtroot, which is a build system for the distribution and it works on Linux, BSD or MacOSX. Next to OpenWrt, IoTBOX also supports Debian Linux.

We design IoTBOX to be able to implement in a single physical machine. Thus we need a virtual network environment in order to connect a physical interface of host machine with many virtual interfaces of QEMU based virtual machines. The following explains how we create a virtual networking environment in a single physical machine.

We first create a virtual switch, which is a multiport Linux bridge [23] that connects physical interface (eth0 of host machine) at one side of the bridge and many different virtual interfaces (eth0 of each virtual machine) at the other side of the bridge. In order to create a virtual switch, we first create a virtual interface br0. As we want host only network, we do not bridge br0 with eth0 right now.

Normally, the br0 interface does not need an IP address as it is supposed to function as a virtual switch. But, in our case, as we would like to manage our virtual switch to take part in layer 3 routing of IP packets, we assign an IP address to it. We assign br0 to a local IP address, which will be the gateway of all virtual machines.

We then try to connect br0 with virtual machines so that packets from a virtual machine can reach br0 and vice versa. But, virtual machines' NIC (eth0 in each virtual machine of Fig. 4) can only process Ethernet frames. In non-virtualized environments, the physical NIC interface (eth0 of host machine) will receive and process the Ethernet frames. It will strip out the Ethernet related overhead bytes and forward the payload (usually IP packets) further up to the OS. With the virtualization however, this will not work since the virtual NICs would expect Ethernet frames. We solve this by using tap interfaces. Tap interfaces are special software entities which tell the physical NIC interface to forward Ethernet frames as it is to virtual NICs. In other words, the virtual machines connected to tap interfaces will be able to receive raw Ethernet frames. We manage a virtual bridge connection of br0 to virtual NICs through tap interfaces by using Linux brctl [24]. We automate all these steps so that the virtual network connection can be done automatically whenever a new virtual machine is added.

Now, br0 is connected to many virtual machines. We have discussed so far about layer 2 level connections. From the viewpoint of layer 3, the br0 interface will be the same network with all virtual machines and it will be the gateway for all virtual machines. The interface, eth0 of host machine will be on a different network and as we do not bridge it directly with br0, we connect br0 and eth0 through NAT (Network Address Translation) managed by *Access Controller*. *Access Controller* implemented by iptables controls all networking related operations such as NAT and outbound traffic from each virtual machine.

IoTBOX as a Stand-alone Multi-architecture Sandbox: In this case, *Access Controller* controls NAT and outbound traffic from each virtual machine such as C&C communication, the DNS resolution and the attack traffic such as DoS. We block all outgoing DoS traffic from malware except allowing some DNS and HTTP



Fig. 5 Observed attacks by IoTBOX.

traffic of a maximum of 5 packets per minute. 23/TCP scans are redirected to *Dummy Server*, which is indeed IoTPOT. In this way, we can monitor how the propagation over Telnet is done.

Analysis Report outputs the results of pcap analysis results for every 24 hours showing total number of packets, the start time and the end time of packet captures, data byte/bite rate, the average packet size and the rate and the total number of a victim IP address for each attack. In addition, commands strings from C&C are summarized if any.

IoTBOX as a High Interaction System in IoTPOT: In this case, *Access Controller* will accept only an incoming connection from *Frontend Responder's* IP addresses and all outbound traffics from high interaction systems except corresponding replies of commands redirected by *Frontend Responder* will be blocked. Please also note that what *Manager* in Fig. 3 is doing is exactly the same as *Access Controller* we have discussed here.

4.2 Analysis Results by IoTBOX

Using IoTBOX, we analyzed 52 selected malware binaries of 8 CPU architectures. Because of limited resources of IoTBOX, malware binary for popular CPU architectures of embedded devices such as ARM, MIPS and MIPSEL focused more in analysis. Please refer to Appendix for the information of analyzed malware samples. Red colored samples show analyzed binaries.

We observed 25 of 52 malware binaries performed 11 different types of DoS attacks and 3 different types of scans such as the Telnet scan and scans on TCP ports such as 23, 80, 8080, 5916 and UDP port such as 123, 3143. The 5 samples cannot be executed because of errors.

A summary of the observed attacks is illustrated in **Fig. 5**. Most attacks we observed were UDP floods and many different types of TCP floods. We also observed UDP floods against multiple

destination ports, which seemed to aim at flooding the target network. Interestingly, we also observed a DNS water torture attack [25], SSL attacks [26] and other two unknown DNS based attacks in which a large number of queries to an unknown type of DNS resource records (RR) were sent to an authoritative name server of a popular ISP. Sample Bin 43 exhibits a unique functionality of a fake web hosting. Namely, it starts hosting a web page that looks like a top page of a popular Chinese search engine "baidu.com." In order to avoid any misuse of the fake web page in a real attack, we carefully monitor if any incoming connections appear although nothing has been seen yet. One more point we notice is that Bin 13, 19, and 22 of Appendix have a backdoor port 5000/UDP open for further remote control of the compromised host because the initial intrusion route, the Telnet, would already have been blocked by iptables during the infection phase to prevent other attackers from compromising the host.

5. Analysis on Attacks

5.1 Overview of Observed Attacks

Figure 6 depicts the overview of Telnet-based attacks observed by IoTPOT and IoTBOX. In order to understand the overview of Telnet attacks observed by our honeypot, we make mappings between different patterns of intrusion and infection behaviors observed by IoTPOT and monetization behaviors observed by malware analysis with IoTBOX. For example, the intrusion pattern "Fixed Order 3," which is shown in Table 2, is always followed by the infection pattern "ZORRO 4," explained in Table 3. Then, infection pattern "ZORRO 4" ends up downloading one of the binaries from certain clusters of binaries that contain common strings, which will eventually exhibit a similar monetization behavior, namely DoS attacks. These mappings reveal that the related patterns and behaviors of attacks can be separated into five major groups, referred to as five corresponding malware families. We also notice that some families seem to spread more aggressively than others. Namely, even within one month of operation, the ZORRO family has updated its Telnet command sequences twice. This family also has increased the diversity of binaries from 7 architectures to 9 architectures dramatically to support more CPU architectures.

Following are our findings.

- We have observed five malware families whose intrusion, infection, and malware binaries are independent from each other.
- 2) From viewpoint of monetization, the different families share the same goal of performing DoS attacks and scans. The only exception is Bin 43 that starts to host a fake search engine.
- 3) Some families seem to spread more aggressively than others. Namely, as in Fig. 6, ZORRO, GAYFGT and nttpd familes have updated command sequences twice during the observation period. Also, the GAYFGT family has increased the diversity of binaries to support more CPU architectures.

5.2 Overview of an Attacking Botnet

5.2.1 Botnet Architectures

Figure 7 shows the overview of a botnet attacking IoTPOT.



Fig. 6 Overview of Observed Attacks by IoTPOT and IoTBOX.

Basically, scanning hosts, we call as Scanners (S), perform Internet wide Telnet scans in order to find hosts listening on Telnet for further infections. After successful Telnet login, the intruding host (I) intrudes the victim sending a sequence of commands over Telnet in order to make the victim machine download the malware binary from a malware download server (D). Downloaded binary is run and after the infection, the victim receives commands from Command and Control Server (C) to perform various DoS attacks and scans. These S, I, D and C can be different hosts or the same host. For example, a single host may perform as (S, I, D) or (D and C) are single host while S and I are different hosts. By analyzing S, I, D and C involving IoTPOT, we found 8 different botnet architectures as follows:

- 1) Botnet relating to the ZORRO family has many host performing scanning only and few I, D and C of different combinations (B1, B2, B3 of Fig. 7).
- 2) Botnet of GAYFGT and *.sh families have many hosts performing both scanning and intruding while D and C are same



Fig. 7 Botnet architectures.

or separate hosts. (B4 and B5 of Fig. 7).

- 3) The propagation of the nttpd family looks alike warm infection in which the attacking host itself is a scanner, an intruder and a malware download server (B6 in Fig. 7). There are also cases in which the scanning and the intruding host make victim infect by sending malware binary over Telnet. In such a case, it is not necessary to download malware binary from a malware download server (B7 in Fig. 7).
- 4) The botnet of KOS family has many hosts performing both scanning and intruding while D and C are separate hosts (B8 of Fig. 7). C can be connected by resolving the "s6.kill123.com" domain. In order to resolve the domain, the authoritative name server IP address of "S6.kill123.com" is hard coded in nttpd malware (bin 44 of Appendix). This authoritative name server is not reachable through normal authoritative name server DNS stacks. In this way, attacker set up an authoritative name server as part of his or her botnet.

6. Related Works

We implemented the first honeypot tailored for IoT devices, IoTPOT, and to the best of our knowledge, there is still no honeypot like IoTPOT that mimics IoT devices of many different CPU architectures while listening on 23/TCP with the ability to learn unknown command interactions. Although Honeyd [22] listens on 23/TCP, it is a low-interaction honeypot and cannot handle not only Telnet options but also command interactions interactively, as explained in Section 3.4.2. Although there is another honeypot known as the Telnet password honeypot [27], its main focus is collecting Telnet password and command interactions are not supported. Other popular low interaction honeypots such as Dionaea [28] and Nepenthes [29] do not support Telnet. Kishimoto et al. [30] propose a novel honeypot that dynamically assigns an IPv6 address to appropriate high interaction honeypots by checking the destination IP address of an incoming NS message which includes the vendor information. SGNET [31] is a honeypot system that has distributed low-interaction sensors to handle known attacks. Its centralized backend high-

interaction honeypots handle unknown attacks redirected from the distributed sensors. The conceptual mechanism of IoTPOT is similar to SGNET and the IPv6 honeypot mentioned above. As in SGNET, Frontend Responder of IoTPOT responds to known attacks and unknown attacks are redirected to IoTBOX. As in the IPv6 honeypot, it tries to deal with different hosts and devices. The main difference between IoTPOT and these existing honeypots is that IoTPOT implements the functionality to perform an automated active scanning of the attacking IP addresses to learn their interactions, namely banner profiles. With this functionality, we can obtain and enrich profiles for presumably vulnerable and infected devices, which is essential for monitoring diverse IoT threats. In other words, IoTPOT learns the banners from vulnerable devices to pretend to be themselves. Moreover, as an initial goal, we highly focus on Telnet attacks which are emerging threats according to the recent observations of darknet as explained in Section 2, emulate the Telnet services of a large variety of IoT devices to attract attacks, and succeed to observe the ongoing attacks to the depth of capturing the malware binaries, which are hardly included in a large malware database like Virus Total. In order to analyze the captured malware binaries, we also implemented IoTBOX, the first sandbox that runs malware of 8 different CPU architectures. Out of more than 15 surveyed sandbox systems in Ref. [32], none support different CPU architecture such as MIPS, ARM.

The main differences of the proposed method against existing works are as follow:

- IoTPOT implements the functionality to perform an automated active scanning of the attacking IP addresses to obtain their banner profiles. With this functionality, we can obtain and enrich profiles for presumably vulnerable and infected devices, which is essential for monitoring diverse IoT threats. In other words, IoTPOT "learns" the banners from vulnerable devices to pretend to be themselves.
- 2) Although the mechanism is similar to existing honeypots, we are the first to focus on a Telnet-based honeypot that can handle banner interactions, authentication interactions and command interactions till the depth of attacks where actual malware binaries can be captured for a detailed analysis.
- 3) We propose IoTBOX, a multi-architecture malware sandbox that is used as a high interaction system as a component of IoTPOT and also independently used as a malware sandbox for analyzing captured binaries.
- 4) We succeeded to report for the first time about details of currently menacing IoT threats targeting vulnerable IoT devices over the world while capturing IoT malware that are hardly included in the existing malware database of Virus Total. We also reveal their monetization behaviors and architectures as botnet.

7. Conclusion and Future Works

We have shown that IoT devices are susceptible to compromises and increasingly are also the target of malware on the masses. We identified five malware families, which show wormlike spreading behavior, all of which are actively used in DDoS attacks.

References

iseclab.org/papers/malware_survey.pdf> (accessed 2015-11-04).

- Cui, A. and Salvatore, J.S.: A quantitative analysis of the insecurity of embedded network devices: Results of a widearea scan (online), available from (http://ids.cs.columbia.edu/sites/default/files/ paper-acsac.pdf) (accessed 2015-05-24).
- [2] Internet Census 212 (online), available from (http://
- internetcensus2012.bitbucket.org/paper.html> (accessed 2015-05-24).
 [3] DailyTech Hackers Use Refrigerator, Other Devices to Send 750,000 Spam Emails (online), available from (http://www.dailytech.com/Hackers+Use+Refrigerator+Other+Devices+to+Send+750000 +Spam+Emails+/article34161.htm) (accessed 2015-05-24).
- [4] Lizard Stresser Runs on Hacked Home Routers Krebs on Security (online), available from (http://krebsonsecurity.com/2015/01/lizardstresser-runs-on-hacked-home-routers/) (accessed 2015-05-24).
- [5] BusyBox (online), available from (http://www.busybox.net/) (accessed 2015-10-30).
- [6] VirusTotal Free Online Virus, Malware and URL Scanner (online), available from (https://www.virustotal.com/) (accessed 2015-05-24).
- [7] Eto, M., Song, J., Nakazato, J., Ohtaka, K. and Nakao, K.: Nicter: A large-scale network incident analysis system: Case studies for understanding threat landscape, *BADGERS '11 Proc. 1st Workshop Build. Anal. Datasets Gather. Exp. Returns Secur* (2011).
- [8] M EL and T L D.: The Carna Botnet Through the Lens of a Network Telescope, Proc. 6th Int. Symp. Found. Pract. Secur. FPS 2003 (Oct. 2013).
- [9] p0f v3 (online), available from (http://lcamtuf.coredump.cx/p0f3/) (accessed 2015-05-24).
- [10] RFC 854 Telnet Protocol Specification (online), available from (https://tools.ietf.org/html/rfc854) (accessed 2015-05-24).
- [11] robertdavidgraham/masscan · GitHub (online), available from (https://github.com/robertdavidgraham/masscan) (accessed 2015-05-24).
- [12] List of applications of ARM cores, Wikipedia, the free encyclopedia. 30-Sep-2015.
- [13] List of MIPS microarchitectures, Wikipedia, the free encyclopedia. 17-Sep-2015.
- [14] PowerPC applications, *Wikipedia, the free encyclopedia.* 18-Dec-2012.
- [15] SuperH, Wikipedia, the free encyclopedia. 30-Sep-2015.
- [16] SuperH RISC engine Family | Renesas Electronics (online), available from (http://www.renesas.com/products/mpumcu/superh/index.jsp) (accessed 2015-11-03).
- [17] netfilter/iptables project homepage The netfilter.org project (online), available from (http://www.netfilter.org/) (accessed 2015-11-03).
- [18] Remote Code Execution in Popular Hikvision Surveillance DVR | Threatpost | The first stop for security news (online), available from (https://threatpost.com/remote-code-execution-in-popularhikvision-surveillance-dvr/109552) (accessed 2015-05-24).
- Index of / aurel32/qemu/mipsel (online), available from (https:// people.debian.org/~aurel32/qemu/mipsel/) (accessed 2015-11-04).
- [20] OpenWrt (online), available from (https://openwrt.org/) (accessed 2015-10-30).
- [21] QEMU (online), available from (http://wiki.qemu.org/Main_Page) (accessed 2015-10-30).
- [22] Developments of the Honeyd Virtual Honeypot (online), available from (http://www.honeyd.org/) (accessed 2015-05-24).
- [23] Linux Bridge and Virtual Networking Blogs by Sriram.
- [24] brctl (online), available from (http://linuxcommand.org/man_pages/ brctl8html) (accessed 2015-11-02).
- [26] DDoS Attacks on SSL: Something Old, Something New (online), available from (http://asert.arbornetworks.com/ddos-attacks-onssl-something-old-something-new/) (accessed 2015-05-24).
- [27] z2c4/telnet-password-honeypot · GitHub (online), available from (https://github.com/zx2c4/telnet-password-honeypot) (accessed 2015-05-24).
- [28] dionaea catches bugs (online), available from (http://dionaea. carnivore.it/) (accessed 2015-05-24).
- [29] home [Nepenthes-finest collection-] (online), available from (http:// nepenthes.carnivore.it/) (accessed 2015-05-24).
- [30] Kishimoto, K., Ohira, K., Yamaguchi, Y., Yamaki, H. and Takakura, H.: An adaptive honeypot system to capture ipv6 address scans, 2012 International Conference on Cyber Security (CyberSecurity), pp.165– 172 (2012).
- [31] Leita, C. and Dacier, M.: SGNET: a worldwide deployable framework to support the analysis of malware threat models, *Dependable Computing Conference, EDCC 2008, Seventh European*, pp.99–109 (2008).
- [32] malware.dvi malware_survey.pdf (online), available from (https://

© 2016 Information Processing Society of Japan

Appendix

As future work, we plan to extend IoTPOT to support more protocols that are likely the target of attacks, such as SSH. Furthermore, we aim to extend the sandbox with capabilities to stimulate even more architectures and environments that are common on IoT devices.

	BinaryID	Filename	Hash(md5)	Architecuture	Date of Capture	Existance in VirusTotal	Detection Ration in VirusTotal	First sub.	Last sub.
	Bin 1	wb.arm	e94f48285ec44e739505889c922def55	ARM	2015/01	YES	0 / 56	1/12/2015 23:50	1/12/2015 23:50
	Bin 2	telnet.arm	4101d096094fa7f3b35a14cee8c5d6bb	ARM	2015/04	NO			
	Bin 3	telnet.m68k	2d4c6238ad43bfcc4668467ef6846196	M68K	2015/04	NO			
	Bin 4	telnet.mp	5c091a1c1311aa37443027a315b663f5	MIPS	2015/04	NO			
ZORRO	Bin 5	telnet.mps	acb79b0810aeb8e1db298cd678b33840	MIPSEL	2015/04	NO			
	Bin 6	telnet.ppc	8e654a673d4bdd8ac16c39f7a4654e1b	Power PC	2015/04	NO			
	Bin 7	telnet.sh4	60ee95389061b1c8ce0cf8b6f748c8a6	SH4	2015/04	NO			
	Bin 8	telnet.sparc	9918dba3e5737d25424b05b9f10b16c0	SPARC	2015/04	NO			
	Bin 9	telnet.x86	792d38b6fdd89d65d35d1b01cd1c2ba7	×86	2015/04	NO			
	Bin 10	arm	f73da5e1e33762f09d74e2d3d16c5c50	ARM	2014/11	YES	7 / 57	1/14/2015 18:30	1/14/2015 18:30
	Bin 11	i586	66113dc9a53866702ac0ca68a9a546b8	1586	2014/11	NO	.,, .,	1717 2010 10	
	Bin 12	1686	6d0f7122a9602007bdb2022c0ca00a3a040b0	286	2014/11	NO			
	Din 12 Din 12	mine	a59a252607042556a77a19b1699d4d01	MIDS	2014/11	VES	6 / 57	2/10/2015 8:41	3/10/2015 8:41
	Din 13	mineal	0000-0000-0000-0000-0000000000000000000	MIDSEL	2014/11	NO	07.57	3/10/2013 8:41	3/10/2013 0.41
	Bin 14	mipsei	a265bab2443e0635a4adte/t4/e069/4	MIF3EL	2014/11	NO			
	Bin 15	sparc	/38db9fbb9debd059/6eaa91bbf1611/	SPARG	2014/11	NO			
	Bin 16	supern	a12e/f5841//fb5d229/0/c5c/f/fa/2	Super H	2014/11	NO			
	Bin 17	arm	06b2fbee4e7ae5c1370753543b7d2e21	ARM	2015/04	NO			
	Bin 18	i586	b7b299fdffbbaabd184ab4d8e69a4d98	x86	2015/04	NO			
	Bin 19	i686	4061432ae8b37171af033d5185b31659	×86	2015/04	NO			
	Bin 20	mips	3fc4bdb902e086e3e5681798036207e7	MIPS	2015/04	NO			
	Bin 21	mips64	feb53f2aec98e96c1321a6811ac05a18	MIPS64	2015/04	NO			
	Bin 22	mipsel	94b2e00fc4c11abd77fb76fd5815d1dc	MIPSEL	2015/04	NO			
	Bin 23	ррс	06940d099751304c704f7a31c2459fb8	Power PC	2015/04	NO			
	Bin 24	sparc	d76cf4f0f37395906df4d2c0defcd923	Super H	2015/04	NO			
	Bin 25	arm	1549aed9b818b6a994dc5fb6c4a57fa2	ARM	2015/04	NO			
GAYFGT	Bin 26	i586	daab490a0a0a0a2b2528b18dacbf66ed	x86	2015/04	NO			
	Bin 27	i686	8a2b06d4ba8b88cab092801fbcbfd8b4	x86	2015/04	NO			
	Din 27	mine	61f32f7a0d4b7641fb03da75af5a1329	MIDS	2015/04	NO			
	Din 20	mips	-74764767-2544-546-44510-5-474	MIDS64	2015/04	NO			
	Bin 29	mips04	ee/d/04/0/c23d4c34be44116a3aa4/d	MIP304	2015/04	NO			
1	Bin 30	mipsei	450500447800303004180104099014be	MIPSEL	2015/04	NU			1
1	Bin 31	ррс	2093e0d093Utc3e5b3345t8cd811d693	Power PC	2015/04	NO			
1	Bin 32	sparc	132c5605/52c9cfcc3f746b8451c7fe6	Super H	2015/04	NO			
1	Bin 33	arm	032ec8869e235bfa8a8dfe7b125a02b6	ARM	2015/05	NO			
1	Bin 34	i586	86f9fc4e914d358d05bd5d1d93a0d673	×86	2015/05	NO			
1	Bin 35	i686	c1ef1dd4232e14c45661e0a8a976867e	×86	2015/05	NO			
1	Bin 36		a41967fbf9a2259ba5551500007b200	MIDE	2015/05	NO			1
1	Dil 30	mips	a+100/1010e2338083555150990/b288c	MIPS	2015/05	NO			
1	Bin 37	mips32	//b/JbUte4a/9dtc284fce55bf3cbe8b	MIPS32	2015/05	NO			
1	Bin 38	mips64	d31261199d16b7ad82e0f87094de6e07	MIPS64	2015/05	NO			
1	Bin 39	mipsel	c652fe5e53cba8c450ee6f7307408c8c	MIPSEL	2015/05	NO			
1	Bin 40	ppc	52f9bd74d63888182fbab15443b70898	Power PC	2015/05	NO			
	Bin 41	sparc	be35cd9d4c6047e940e6c58a96fbf0b8	SPARC	2015/05	NO			
nttnd	Din 41 Din 42	optio	bbf1327c1a5213b41a4d22c4b4806f7c	MIDSEL	2015/05	VES	0 / 57	2/12/2015 17:24	2/20/2015 15:17
KOS	Din 42	1225 9106	as291bb56b92b160b1ab402917091a1	MIDS	2015/05	NO	07.51	2/18/2013 17/24	3/20/2013 13.17
K03	Bin 43	1220.0190	02020 1003010301030100049381708101	WIF 3	2015/05	NO			
nttpa	Bin 44	nttpa	d9/9/200101420/65003a16150664306	1511	2015/06	NO			
	Bin 45	armp	dec3b1949C3b10/dc3a9/3015269edd6	ARM	2015/06	NU			
	Bin 46	mipselp	6/abda/e85c838448ca1f/915dfc6b1/	MIPSEL	2015/06	NO			
	Bin 47	mipsp	de31e34c2e5f6198026354704ac00e54	MIPS	2015/06	YES	2 / 57	6/2/2015 19:44	6/2/2015 19:44
	Bin 48	ррср	4dcfba3c38863e647162ff81f37e8eb8	PPC	2015/06	YES	2 / 57	6/2/2015 19:40	6/2/2015 19:40
	Bin 49	shp	afcda120ec94869329e2b27a9c0e61fc	SH4	2015/06	YES	4 / 57	6/2/2015 19:35	6/3/2015 6:59
+.sn	Bin 50	armm	1c435276ffabe48d753527cccfe398a4	ARM	2015/06	YES	6 / 56	6/1/2015 7:48	6/1/2015 7:48
	Bin 51	mipselm	fe1e5c05fb6abe21f9075a13ea0bec79	MIPSEL	2015/06	YES	3 / 56	6/1/2015 7:48	6/1/2015 7:48
	Bin 52	mipsm	1616d1cca4ccbca38f8948a42c99239c	MIPS	2015/06	YES	7 / 57	6/1/2015 7:49	6/5/2015 8:34
	Bin 53	ppcm	ac86a5a187f38d9d19c482bbbf24f148	PPC	2015/06	YES	2 / 56	6/1/2015 7:48	6/1/2015 7:48
	Bin 54	shm	d0173b706f9c65c1f011d4683a68217d	SH4	2015/06	YES	4 / 56	6/1/2015 7:47	6/1/2015 7:47
	Bin 55	568i	6bb6edd07979e547dc528a2143a9bf4f	x86	2015/06	NO	.,		
	Bin 56	669;	3ead0f86731993fc8cf4f94159805990	×86	2015/06	NO			
	Din 50	0001	b5665975ac7ab4(000294146c9bb6794	MIDSEI	2015/00	NO			
	Bin 37	eiimps	617-01065-6100-576074hJ660076	WIF GLL	2015/06	NO			
	Bin 58	nusper	11/a6100ta6129C3aa/t3/4bed0t92/6	Super H	2015/06	NU			
	Bin 59	mar	2/030/434et9/c688b831bc2806/1886	ARM	2015/06	NO			
	Bin 60	рср	129b0be5bf9008095939db8da7c34d4e	Power PC	2015/06	NO			
GAYFGT	Bin 61	racps	b39b75d52dee457ccc825749226ec8e3	SPARC	2015/06	NO			
	Bin 62	sipm	5f68776702514580793aac478aadb811	MIPS	2015/06	NO			
	Bin 63	a	f47b27ed72f1a84f43d154399c04aca6	ARM	2015/06			6/13/2015 15:16	
	Bin 64	m	000001 541 400 400 0 50 101 44 17 044	1000		YES	10 / 57		6/13/2015 15:16
	Bin 65		33899bt41499403c3a53cd3b44d7a844	MIPS	2015/06	YES NO	10 / 57		6/13/2015 15:16
	Din 66	mi	16679aa6674968494ae32f45fe2025e3	MIPS	2015/06 2015/06	YES NO NO	10 / 57		6/13/2015 15:16
	I DILLOU	mi	338990741499403c3a53cd3b44d7a844 16679aa6674968494ae32f45fe2025e3 0d52132275d204363df8b29eb379a2ea	MIPS MIPSEL Power PC	2015/06 2015/06 2015/06	NO NO NO	10 / 57		6/13/2015 15:16
	Bin 67	mi p s	338990741499403c3a53c30304407a844 16679aa6674968494ae32f45fe2025e3 0d52132275d204363df8b29eb379a2ea ffea6ec00f8ab522ee1e73ab8d4a936b	MIPS MIPSEL Power PC SH4	2015/06 2015/06 2015/06 2015/06	VES NO NO NO	10 / 57		6/13/2015 15:16
	Bin 67 Bin 68	mi p s ayy.arm	33899014149340253832603044073844 16679aa6674968494ae32f45fe2025e3 0d52132275d204363df8b29eb379a2ea ffea6cc00f8ab522ee1e73ab8d4a936b 112baeed64abe8f73e22664c53d30f40	MIPS MIPSEL Power PC SH4 ARM	2015/06 2015/06 2015/06 2015/06 2015/06	YES NO NO NO NO NO	10 / 57		6/13/2015 15:16
	Bin 60 Bin 67 Bin 68 Bin 69	mi p s ayy.arm ayy.m68k	338990741499403538356339473844 166798a6674968494ae3274476202563 0d52132275d204363df8b29eb379a2ea ffea6ec0076ab522ee1e73ab8d4a936b 112baeed64abe8f73e22664c53d30f40 6f35aefa8cd78b2c9dcd814a0129bfrl3	MIPS MIPSEL Power PC SH4 ARM M68K	2015/06 2015/06 2015/06 2015/06 2015/06 2015/06	YES NO NO NO NO NO	10 / 57		6/13/2015 15:16
	Bin 60 Bin 67 Bin 68 Bin 69 Bin 70	mi p s ayy.arm ayy.m68k	3389901114994U3c3a353C63044078444 16679aa6674968494as32f45fe2025e3 0d52132275d204453df8b29eb379a2ea ffea6ec00f8ab522ee1e73ab8d4a936b 112baeed64abe8f73e22664c53d30f40 6f35aefa8cd78b2c9ded814e0129bfd3 200h9b23986e922856d756f632142670	MIPS MIPSEL Power PC SH4 ARM M68K MIPS	2015/06 2015/06 2015/06 2015/06 2015/06 2015/06	YES NO NO NO NO NO NO	10 / 57		6/13/2015 15:16
	Bin 60 Bin 67 Bin 68 Bin 69 Bin 70 Bin 71	mi p s ayy.arm ayy.m68k ayy.mp	3389907114994U3c38353C605044678844 16679aa6674968494ac3247676202563 Od52132275d204563df8b29eb379a2ea ffea6ec00f8ab52zei e 73ab5d48336b 112baecd64be873e22664c55330f40 6f35aefa8cd78b2c9ded814e0129bfd3 20fb9b239866922856d256f6321d2670 70f75280ba31169329d45c1456a2	MIPS MIPSEL Power PC SH4 ARM M68K MIPS MIPSEI	2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06	YES NO NO NO NO NO NO	10 / 57		6/13/2015 15:16
	Bin 60 Bin 67 Bin 68 Bin 69 Bin 70 Bin 71 Bin 72	mi p s ayy.arm ayy.m68k ayy.mp ayy.m	3.369/0711 (19394)0.53.633.00.05.07447/3644 166739a667346844a.6274476220563 0452132275420453.6180529b.5798.26a 172bare.db4ab.e073342264455340340 112bare.db4ab.e073342266455340340 16735aefa8c073b24265445564236476 16735aefa8c073b24265642567632142670 70775260ba31199322903ace1306e698 407647293200b14729-441193743-378444	MIPS MIPSEL Power PC SH4 ARM M68K MIPS MIPSEL Power PC	2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06	YES NO NO NO NO NO NO NO NO NO	10 / 57		6/13/2015 15:16
	Bin 60 Bin 67 Bin 68 Bin 69 Bin 70 Bin 71 Bin 72 Bin 72	mi p s ayy.arm ayy.m68k ayy.mp ayy.mp ayy.ppc	3.3899071 (1994)03:383:0030940/1844 16679aa661796844a.62/456:202563 04521322754204563/t6529b.57932ea fraa6cc0078ab522ea (e 73ab8d4a936b 1128aeedd4abe873e22664c53430/40 6735aefa8cJ78b.294edd14e0129brt3 20fb.9b23986c922856d256f6321d2670 70775260ba3119932229d32ea (d06e698 40:3e23090e1ad22e4118336e325d44 40:3e23090e1ad22e4118336e325d44	MIPS MIPSEL Power PC SH4 ARM M68K MIPS MIPSEL Power PC SH4	2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06	YES NO NO NO NO NO NO NO NO	10 / 57		6/13/2015 15:16
	Bin 60 Bin 68 Bin 69 Bin 70 Bin 71 Bin 72 Bin 73 Bin 73	mi p s ayy.arm ayy.m68k ayy.mp ayy.mp ayy.pc ayy.sh4	3.3699071 (19340.35.03.05.04747.3644 16573a.667.36684.a5.2476.52205.3 0.452.1322.75.42045.34785.296.3739.26.a (1126a.ec.0780.5220 et 7.3.30.64439.36.b 1125a.ec.064.35.2644.53.430140 6735a.ec.084.738.22644.53.430140 6735a.ec.084.738.22644.533.44012.94613 207b9.23.2366.ec.92256.642.5676.321.467.0 7077520.063.1799.22943.3c.a1.056.698 400.362.3020.061.827.441.432.632.53644 450.389.333.6577.44.44.4208.23664.113 13.042.9878.04281.1.2711.4.2015.1.167.1	MIPS MIPSEL Power PC SH4 ARM M68K MIPS MIPSEL Power PC SH4 SDAP	2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06	YES NO NO NO NO NO NO NO NO NO	10 / 57		6/13/2015 15:16
70550	Bin 60 Bin 67 Bin 68 Bin 70 Bin 70 Bin 71 Bin 72 Bin 73 Bin 74 Bin 75	mi p s ayy.arm ayy.m68k ayy.mp ayy.mp ayy.ppc ayy.sh4 ayy.sparc	338907114994035383050874017844 16579aa66794844a-8274576222653 0d52132275420453347852945379326a 1122baed64548494352145139326 1122baed64548673822664553430740 6735acf8637825266425673247214670 70775280ba31993229453ce1406e688 40c3e23080e1a52ce4418336e32548 40c3e23080e1a52ce4418336e32548 4132692580834938811a3711b2294554 412780115ac9311a-70-b259354	MIPS MIPSEL Power PC SH4 ARM M68K MIPS MIPSEL Power PC SH4 SPARC vP ^e	2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06	YES NO NO NO NO NO NO NO NO NO NO NO	10 / 57		6/13/2015 15:16
ZORRO	Bin 67 Bin 68 Bin 69 Bin 70 Bin 71 Bin 72 Bin 73 Bin 74 Bin 75 Bin 75	mi p s ayy.arm ayy.m68k ayy.mp ayy.mp ayy.ppc ayy.sh4 ayy.sparc ayy.x86	3.3899071 19394032.833.0030447.844 16573aa667.84684a.632445-022653 0.45213227.5420453.818529b.5739.26a 112bace0748.052281e 17.330.8443.936b 112bace0748.052646134.01298/13 20fb.9523986.92285642564632142670 7077526043114912298163 20fb.9523986.9228564256632142670 707752609318126211298/13 20fb.9523986.9228564256632142670 70752609318126211286433 1462.6223020612898116.37112-2845544 7477807115cec43318670.0055239.84641 747807115cec43318670.0055239.8464	MIPS MIPSEL Power PC SH4 ARM M68K MIPS MIPSEL Power PC SH4 SPARC x86 ADM	2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06	YES NO NO NO NO NO NO NO NO NO NO NO	10 / 57		6/13/2015 15:16
ZORRO	Bin 67 Bin 68 Bin 69 Bin 70 Bin 71 Bin 72 Bin 73 Bin 74 Bin 75 Bin 76 C T	mi p s ayy.arm ayy.m68k ayy.mp ayy.mp ayy.ppc ayy.sh4 ayy.sparc ayy.x86 scanner.arm	33699071 (1994035363505054471844 16573a667396844a6274675202653 0d521322754204533478529b5739a2ea 112baeed64abe8773e22684c53430140 6735aefabc378b229b632782146370 70775208ba316922586425673214670 70775208ba316922586425673214670 70775208ba316922956425673214670 70775208ba316922956425673214670 70775208ba316922956425673214670 70775208ba31672441183366325684 40c3e2308051a62741183366325684 4163243446321897063126239ab44 145224334469977631262aee6baa21e 41632434469977631262aee6baa22	MIPS MIPSEL Power PC SH4 ARM M68K MIPS MIPSEL Power PC SH4 SPARC x86 ARM ARM	2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06	YES NO NO NO NO NO NO NO NO NO NO	10 / 57		6/13/2015 15:16
ZORRO	Bin 67 Bin 68 Bin 69 Bin 70 Bin 71 Bin 72 Bin 73 Bin 74 Bin 75 Bin 76 Bin 77	mi p s ayy.arm ayy.m68k ayy.mp ayy.mp ayy.ppc ayy.sh4 ayy.spac ayy.sh4 scanner.arm scanner.m68k	33890711499403538305087407844 16579aa667948644a-827456220563 0d5213227542045634165294b37932ea fraadeco0768ab522ea1e73ab8d4a936b 112aeaed04abe873e22664553430140 6735aef380378b229de314e0129b1d3 07075280ba31f93229db3ce1406698 40c3e23080e1ad22e4118336e325684 40c3e23080e1ad22e4118336e325684 40c3e23080e1ad22e4118336e325684 13ae92a808394938811a3711b2e9d5b4 7477801135ced3319a721822e86b42 7473801135ced3319a721822e86b43 143526334463972781222e86b4a21e 63eed54306e2684711b40b38e08651	MIPS MIPSEL Power PC SH4 ARM M68K MIPSEL Power PC SH4 SPARC x66 ARM M68K	2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06	YES NO NO NO NO NO NO NO NO NO NO NO NO NO	10 / 57		6/13/2015 15:16
ZORRO	Bin 67 Bin 68 Bin 69 Bin 70 Bin 71 Bin 72 Bin 73 Bin 74 Bin 75 Bin 76 Bin 77 Bin 78	mi p s ayy.arm ayy.m68k ayy.m6 ayy.m6 ayy.sh4 ayy.sh4 ayy.sh4 scanner.m68k scanner.m68k	33693071 19394035383003054473844 16573ae673968494ae32445022653 0452132275420453348529b5739a2ea 112baee40978522e1 673ab8443936b 112baee40978522e1 673ab8443936b 112baee4047852261493204534 112baee4047852261492678214870 112baee4047825261484 112baee40478254784 112baee40478254784 112baee4047845478 112baee4047845478 112baee4047816923984 112baee4047816923984 112baee4048975812628984 112baee404975812628984 112baee404975812628984 112baee404975812628984 112baee404975812628984 112baee404975812628984 112baee404975812628984 112baee404975812628984 112baee404975812628984 112baee404975812628984 112baee404975812628984 112baee404975812628984 112baee404975812628984 112baee404975812628984 112baee404975812628984 112baee404975812628984 112baee404975812628984 112baee404975812628984 112baee404975812628984 112baee404975884 112baee404975884 112baee404975884 112baee404975884 112baee404975884 112baee404954570168968968368240633 112baee405380584 112baee40545470168968368240633 112baee405389584 112baee405389584 112baee40545470168968368240633 112baee405389584 112baee40545470168968368240633 112baee405389584 112baee40545470168968368240633 112baee405389584 112baee405389584 112baee40545470168968368240633 112baee405389584 112baee40545470168968368240633 112baee405389584 112baee405389584 112baee40545470168968368240633 112baee405389584 112baee405454701689584 112baee405454701689584 112baee405454701689584 112baee405454701689584 112baee405454701689584 112baee405454701689584 112baee4054547016804 112baee40545470168954 112baee40545470168954 112baee40545470168954 112baee40545470168954 112baee40545470168954 112baee40545470168954 112baee40545470168954 112baee40545470168954 112baee40545470184 112baee40545470184 112baee40545470184 112baee40545470184 112baee40545470184 112baee40545470184 112baee40545470184 112baee40545470184 112baee40545470184 112baee40545470184 112baee40545470184 112baee40545470184 112baee40545470184 112baee40545470184 112baee404545470184 112baee404545470184 11	MIPS MIPSEL Power PC SH4 ARM M68K MIPS MIPSEL Power PC SH4 SPARC x86 ARM M68K MIPS	2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06	YES NO NO NO NO NO NO NO NO NO NO NO NO NO	10 / 57		6/13/2015 15:16
ZORRO	Bin 67 Bin 68 Bin 69 Bin 70 Bin 71 Bin 72 Bin 73 Bin 74 Bin 75 Bin 76 Bin 77 Bin 78 Bin 79	mi p s ayy.arm ayy.m68k ayy.m68k ayy.m6 ayy.ppc ayy.sh4 ayy.sparc ayy.x86 scanner.arm scanner.m68k scanner.mps	33898071 (199403538305085407)84 16573aa67396844a-8274576222653 0d5213227542045334852945379326a 1122aead64364293621 (199226453430740 6735aef8637882328614-01295143 120509523986-02258662567632146270 70775280ba31993229453c=14064688 40c3e23080e1a452c4418336e32548 40c3e23080e1a452c4418336e32548 40c3e23080431997209453c=14064688 40c3e230804392781262ee46ba214670 13ae9280839493811a3711b2e4554 147807115cea3219e7b04552339b44 14522433446592761262ee46ba21e 63cec45300c28614717b40b33cc0a551 147c0424577016958861835240c33 73a421e470ab43642c53761262ee45ba21e6883	MIPS MIPSEL Power PC SH4 ARM MIBK MIPSEL Power PC SH4 SPARC x86 ARM M68K MIPS MIPSEL	2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06	YES NO NO NO NO NO NO NO NO NO NO NO NO NO	10 / 57		6/13/2015 15:16
ZORRO	Bin 67 Bin 68 Bin 69 Bin 70 Bin 71 Bin 72 Bin 72 Bin 73 Bin 74 Bin 75 Bin 76 Bin 77 Bin 78 Bin 79 Bin 80	mi p s ayy.arm ayy.m68k ayy.m68k ayy.m68k ayy.m6 ayy.sh4 ayy.sh4 ayy.sh4 ayy.sh4 scanner.arm scanner.m68k scanner.mps scanner.mps	3.3693071 (19340.35.03.50.05.04.47.36.44 16573a.667.36684.a5.247.65.220.53 0.452.1322.75.420.45.34.05.29.65.73.92.6a 11.2b.nec.054.a5.20.26.17.33.06.44.93.95.0 11.2b.nec.054.a5.20.26.17.33.06.44.93.95.0 11.2b.nec.054.a5.20.46.01.24.01.29.07.03 12.25.20.06.21.25.20.46.01.24.01.29.07.03 12.25.20.06.21.25.25.24.02.01.03 12.25.25.25.25.25.25.25.25.25.25.25.25.25	MIPSEL Power PC SH4 ARM M68K MIPSEL Power PC SH4 SPARC x86 ARM M68K MIPSEL Power PC	2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06	YES NO NO NO NO NO NO NO NO NO NO NO NO NO	10 / 57		6/13/2015 15:16
ZORRO	Bin 60 Bin 68 Bin 68 Bin 69 Bin 70 Bin 71 Bin 71 Bin 72 Bin 73 Bin 74 Bin 75 Bin 76 Bin 75 Bin 76 Bin 77 Bin 78 Bin 78 Bin 79 Bin 80 Bin 81	mi p s ayy.arm ayy.m68k ayy.mp ayy.mb ayy.pc ayy.sh4 ayy.sparc ayy.sh4 scanner.mbs scanner.mps scanner.mps scanner.sh4	3.369/0711 (1994)03:363:0030474/3644 1673aa673/06844a.62/476/5202563 0d52132273;020453.3fb529eb379a2ea freade.0078b5229e1 (733b842443930b 112baeed64abe8f73e22664c53430f40 6f35aef8e3d78b229eb3742214270 707752620b331692236642567632142670 707752620b331692204532142670 707625308051432256642567632142670 707752630b3149220451332142670 70775263345714464202063664113 13ae92830839495381163711b2e9d5b4 14b324d3344c6927c812c2eee8baa21e 63ec643306c28454711b4b03ac0a5651 1447c024237011668:9386872393b4d4 14b324d3344c6927c812c2eee8baa21e 63ec643306c28454711b4b03ac0a5651 1447c024457101680:93868724240c33 73ad21e470ab43da2aab39f621f6683 65b0feec4e28276141ec0ba38cf21aaa	MIPS MIPSEL Power PC SH4 ARM M68K MIPS MIPSEL Power PC SH4 SPARC x86 ARM M68K MIPS MIPSEL Power PC SH4	2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06	YES NO NO NO NO NO NO NO NO NO NO NO NO NO			6/13/2015 15:16
ZORRO	Bin 60 Bin 68 Bin 68 Bin 69 Bin 70 Bin 71 Bin 71 Bin 72 Bin 73 Bin 74 Bin 75 Bin 76 Bin 76 Bin 77 Bin 78 Bin 78 Bin 79 Bin 80 Bin 81 Bin 81	mi p s ayy.arm ayy.mb8k ayy.mp ayy.ppc ayy.sh4 ayy.sparc ayy.sh4 ayy.sparc scanner.arm scanner.mps scanner.mps scanner.mps	3.369/071 (1994)03:033:0030447/3644 (1673aa67346844ao2/44562205a3 0.4521322754204533(18529b5739a2ea (172bace0768b222e1 e733ab6443936b 112bace0764b222e1 e733ab6443936b 112bace074b22964c35340267 1255acf38c478b22964c354401294643 1267bb23966e229564256763214670 70775208ba31(1992294b32) 405c223090e1 ad22441133562325484 45c329392452938114371142e3554 1475807115cecd3219e7b0455239abd4 1452243344649776412e2655439abd4 1452343444639776412c2ee65baa21e 56b0fecc4e28276141cc0b9386721663 56b0fecc4e28276141cc0b9386721663 56b0fecc4e28276141cc0b9386721663 56b0fecc4e28276141cc0b9386721663 56b0fecc4e28276141cc0b9386721aa	MIPSEL Power PC SH4 ARM M68K MIPSEL Power PC SH4 SPARC x86 ARM MIPSEL Power PC SH4 SPARC x86 ARM MIPSEL Power PC SH4 SH4	2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06	YES NO NO NO NO NO NO NO NO NO NO NO NO NO			6/13/2015 15:16
ZORRO	Bin 60 Bin 61 Bin 68 Bin 70 Bin 71 Bin 71 Bin 72 Bin 72 Bin 73 Bin 74 Bin 75 Bin 76 Bin 77 Bin 78 Bin 79 Bin 80 Bin 81 Bin 82 Bin 83	mi p s ayy,arm ayy,m68k ayy,mp ayy,mp ayy,ppc ayy,shd ayy,spac ayy,x86 scanner,m6% scanner,m6% scanner,m9p scanner,m9p scanner,sh4 scanner,sh4 scanner,sh4 scanner,sh4	3.3699071 (19940.35.03.50.50.4747/3644 16973aa67.946844a.627467c2205a3 0d52132275420453affb329b.379a2ea freade.0076b.3222e1 (73.30.8443.93b) 112baee.d64abe8773e22664c53430f40 6f33aef18e3078b229be37444393b) 112baee.d64abe8773e22664c53430f40 6f33aef18e3078b229b63246702 107075203ba31f99322943b324 140129f163 107075203ba31f99322943521 4870 70775203ba31f99322943521 4870 70775203431920452586236f1623239b44 4453243344c69770185e3845427339b44 1453243344c69770185e3845427186835a2440c33 73ad2144710a836a244113436a5a2406511 147c04243701169e3894838a2440c33 73ad214470a8342a21917201272689736121aa 493cb7844707378b13ac049342e0f4512aa 493cb7844707378b13ac049342e0f4512aa 493cb7844707378b13ac049342e0f4512aa	MIPS Power PC SH4 ARM M68k MIPS MIPS MIPS SH4 SH4 SPower PC SH4 SPARC x86 ARM M68K MIPS Power PC SH4 SPARC SH4 S6 ARM M68K MIPS SH4 X66 ARM X66 ARM	2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06	YES NO NO NO NO NO NO NO NO NO NO NO NO NO			6/13/2015 15:16
ZORRO	Bin 60 Bin 61 Bin 68 Bin 70 Bin 71 Bin 73 Bin 73 Bin 74 Bin 75 Bin 76 Bin 78 Bin 78 Bin 78 Bin 78 Bin 81 Bin 81 Bin 82 Bin 83 Bin 84	m p s ayy.arm ayy.m68k ayy.mp ayy.ppc ayy.sh4 ayy.sparc ayy.sh4 scanner.m68k scanner.m68k scanner.m68k scanner.m68k scanner.m68k scanner.m84 scanner.sh4 scanner.sh4 scanner.x86 a m	3.3690071 (1994)033.033.0030447/3644 16973aa667346844a.032445-022653 0.d521322754204533(18)296379a2ea (1986)0078052261 (73.308643936) 112bae0454ab6773e2264613401298/d3 20769b23986.0329564256425343040 20769b23986.0329564256632142670 70775260b31(192240361441298/d3 20769b23986.0329564256632142670 7077526093381-037114298/d3 20769b23986.0329564256632142670 7077526939381-037114298/d3 20769b23986122561226286425 14632434412983981-137114294554 1473204152c6312768122c2ee65baa21e 6560540c2626864711b60b366239abd635 56005ec4282276141c0b9366721683 56605ec4282276142c093966121683 56605ec428227614266971614284064f 653292ffe24c796573229b068646339 bcb87098610027322e56971614e557	MIPS MIPSEL Power PC SH4 ARM M68K MIPS MIPSEL Power PC SH4 SPARC x86 ARM MIPS SH4 MIPSEL Power PC SH4 x86 ARM MIPS	2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06	YES NO NO			6/13/2015 15:16
ZORRO	Bin 60 Bin 61 Bin 68 Bin 69 Bin 70 Bin 71 Bin 72 Bin 71 Bin 72 Bin 73 Bin 74 Bin 75 Bin 76 Bin 77 Bin 78 Bin 79 Bin 80 Bin 81 Bin 82 Bin 84 Bin 85	mi p s ayy.arm ayy.m68k ayy.mp ayy.m68k ayy.mp ayy.mp ayy.sh4 ayy.sparc ayy.x86 scanner.m68k scanner.m68k scanner.m68k scanner.m68k scanner.m9 scanner.m9 scanner.sh4 scanner.sh4 scanner.sh4 mi	3.369/0711 (1994)03:033:030.0304407/844 16973ae67349644ae32446522053 0.452132273;0204533(48)29b;379a2ea 112baea0036220e1 (73308443936) 112baea04782;22614733080443936) 112baea04782;22664255430460 1035aefae378262565226652166732142670 707752080e3119922930532140 0.45239208-01321927036232484 45ca89a393a657(a4a4;4208;3664113 13ae92480334453119e70a552393b44 143520434446937:0812;22ae605ha2166 147;604154254701659;8294638a;240;33 73ac2144710at53239b45 147;604214554701659;8294638a;240;33 73ac2144710at534204531972 1560576;4222271411;400539304014 1432043444;63770169;8294638a;240;33 73ac2144710at534264711ab0342;0405121aa 433a;24947107378611aad0433a;2605121aa 433a;24947107378611aad0433a;2614683 3560566;4222572141;40053936211aa	MIPS MIPSEL Power PC SH4 ARM M68K MIPS MIPSEL SH4 SPARC SH4 SPARC X66 ARM M68K MIPS MIPSEL SH4 X66 ARM X68 ARM MIPSEL	2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06	YES NO NO			6/13/2015 15:16
ZORRO	Bin 60 Bin 61 Bin 68 Bin 70 Bin 71 Bin 71 Bin 73 Bin 73 Bin 73 Bin 73 Bin 73 Bin 73 Bin 76 Bin 77 Bin 78 Bin 78 Bin 80 Bin 81 Bin 82 Bin 83 Bin 84 Bin 86	m p s ayy.arm ayy.m68k ayy.mp ayy.ppc ayy.sh4 ayy.sparc ayy.sh4 scanner.m68k scanner.m68k scanner.m68k scanner.m68k scanner.m68k scanner.m84 scanner.sh4 scanner.sh4 scanner.sh4 scanner.sh4 scanner.sh4	3.3899071 193940.35.035.005447/3644 16573ae673.46844a.62/45/622026-3 0.d5213227.5420453.478529b.579a2ea 172bace0763b.2282e1 673ab6443936b 112bace0764b.22864615340129brd3 20fb9b23986.62285642564632102670 20f53aef8acf78b.2286461340129brd3 20fb9b23986.6228564256f632102670 20f53aef8acf78b.228461430129brd3 20fb9b23986.6322564256f632102670 20f53aef8acf78bc78bc784 20fb9b23986.632858116371142.94554 14632430461927.63122.6286421 146324461927.63122.6286421 145324454701659.2896818_32742954 145324454701659.28968382421e5 56b0fec4282276112ce039366171a 3463cr59470736b134004321683 56b0fec42822761412cb9396671a 3463cr594707378b1340043404643 20f3278613404698659216683 56b0fec4282276141cb03936671a 181411bec4473486996659219407 40624553246ec299863340543911 405253246ec2998633405343911 40625455246ec2998633405343911 406246532466c299867513343429146073	MIPS MIPSEL Power PC SH4 ARM M68K MIPSE SH4 SPARC SH4 SPARC X86 ARM M68K MIPSEL Power PC SH4 X86 ARM MIPSEL X86 ARM MIPS SH4 X86 ARM MIPS	2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06	YES NO NO			6/13/2015 15:16
ZORRO	Bin 60 Bin 61 Bin 68 Bin 69 Bin 70 Bin 71 Bin 71 Bin 72 Bin 73 Bin 74 Bin 75 Bin 76 Bin 76 Bin 77 Bin 78 Bin 79 Bin 80 Bin 82 Bin 82 Bin 84 Bin 85 Bin 87	mi p s ayy.amg ayy.m68k ayy.m68k ayy.m68k ayy.m68k ayy.sparc ayy.sh4 ayy.sparc ayy.sh4 scanner.m68k scanner.m68k scanner.m68k scanner.m68k scanner.m68k scanner.sh4 a mi ppc sh	3.369/0711 (19340.35.03.50.05.04.71.844 16573aa667.94684.as.22445.0226.53 0.452.1322.75.420.453.34105.29.b.579a.2e.a 17.2b.nec.054.as.252.et ir 7.3a.0844.93.95.b 11.2b.nec.054.as.252.et ir 7.3a.0844.93.95.b 11.2b.nec.054.as.252.et ir 7.3a.0844.93.95.b 11.2b.nec.054.as.252.et ir 7.3a.0844.93.95.b 11.2b.nec.054.042.95.042.95.052.142.07.03 10.2b.nec.054.042.95.042.95.052.142.07.03 10.2b.nec.054.042.95.052.052.052.052.052.052.052.052.052.05	MIPS Power PC SH4 ARM M68K MIPS MIPSEL Power PC SH4 SPARC x86 ARM M68K MIPS MIPSEL Power PC SH4 SPARC x86 ARM MIPSEL Power PC SH4 X86 ARM MIPS MIPS MIPS PSEL POWER PC SH4	2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06	YES NO NO			6/13/2015 15:16
ZORRO	Bin 60 Bin 61 Bin 62 Bin 63 Bin 70 Bin 71 Bin 72 Bin 73 Bin 73 Bin 73 Bin 73 Bin 73 Bin 76 Bin 77 Bin 78 Bin 80 Bin 81 Bin 82 Bin 83 Bin 84 Bin 87 Bin 78 Bin 79	mi p s ayy,arm ayy,m68k ayy,m68k ayy,m68k ayy,sparc ayy,sh4 ayy,sparc ayy,sh4 scanner,m68k scanner,m68k scanner,m68k scanner,sh4 scanner,s	3.3899071 193940.35.835.005447.847 16573aa673.46844a.632456-202563 0.d5213227.5520453.318529b.379a2ea 1728.ee.0078.05228e1 673.3062443.936b 1128.ee.0644a.9573e2264613.40129k103 20fb.9bc23986.e5228564256f632142670 707752604311931229b.352142670 20fb.9bc23986.e5228564256f632142670 707752693831.6321142.94103 20fb.9bc239386.952464153 1052.6232030e1.6322.44118356.2526344 465.2829303.65776.43424208.3564173 148524634446939811.6371142.945544 148524634446939811.6371142.945544 14852463444693776312.264ene6baa.21e 14852463444693776312.264ene6baa.21e 14852463444693776812.2649544 148524537061736153.264968356247663 556006ec4282276141c0.6939.6671aa 34631-7949777378611.36403430404f ffc.3229247.247.96573229.b0.68468933 16.141b.0e4472.8486966.694219407 4062165322.65669.711a46272.866.079 2.51445aad532.6266471445374021 405214532.2666.079 2.51445aad532.6269577483.2774021 2.51445aad532.62695774383274021 2.51445aad532.62695774383274021 2.51445aad532.62695774433274021 2.51445aad532.62695774383274021 2.51445aad532.626957748337474021 2.51445aad532.6269577485374021 2.51445aad532.62695774453774021 2.51445aad532.62695774453774021 2.51445aad532.626954774853774021 2.51445aad532.626954774853774021 2.51445aad532.626954774853774021 2.51445aad532.626954774853774021 2.51445aad532.626954774853774021 2.51445aad532.626954774853774021 2.51445aad532.626954774853774021 2.51445aad532.626954774853774021 2.51445aad532.626954774853774021 2.51445aad532.626954774853774021 2.51445aad532.6569774853774021 2.51445aad532.6569774853774021 2.51445aad532.6569774853774021 2.51445aad532.6569774853774021 2.51445aad532.6569774853774021 2.51445aad532.6569774853774021 2.51445aad532.6569774853774021 2.51445aad532.656774853774021 2.51445aad532.6567757133427485774021 2.51445aad532.65774853774021 2.51445aad532.65774853774021 2.51445aad532.65774853774021 2.51445aad532.65774853774021 2.51445aad532.65774853774021 2.51445aad532.65774853774021 2.51445aad53547545774853774021 2.514454343845774853774021 2.51445434384577485374	MIPS MIPSEL Power PC SH4 ARM M68K MIPSEL Power PC SH4 SPARC x86 ARM M68K MIPSEL Power PC SH4 SFH4 M68K MIPSEL Power PC SH4 X86 MIPSEL Power PC SH4 X86 ARM MIPSEL PDE SH4 SPC SH4 ARM MIPS SH4 SPC SH4	2015/06 2015/06	YES NO NO			6/13/2015 15:16
ZORRO	Bin 60 Bin 61 Bin 69 Bin 70 Bin 71 Bin 71 Bin 71 Bin 72 Bin 73 Bin 74 Bin 75 Bin 76 Bin 76 Bin 77 Bin 78 Bin 81 Bin 81 Bin 82 Bin 84 Bin 85 Bin 87 Bin 88 Bin 88	mi p s ayy.amm ayy.m68k ayy.mp ayy.m68k ayy.mp ayy.m68k ayy.mp ayy.ma ayy.sha ayy.sha scanner.m88k scanner.m80k scanner.m8	3.369/0711 (19394)03:033:00300447/3644 1673aa67346844ao2/445622053 0.d521322754204533(18529b;57)9a2ea freadec0078b;522e1 e73ab8443936b 112baec6074b;522e1 e73ab8443936b 112baec6074b;52964c53430140 6735aefa8c778b;294ed814e0129th33 207b9523966e5225664256f3214670 70775200b;32966e522566256f3214670 70775200b;329656256725471b;60265239ab4 465a986334657Ca444c4208c36641f3 13ae92a808394958811e3711b;2e955b4 7477807115cce32319e70a55239ab44 14326434463027c812c2ee65baa21e 65326976c24571b;603664533 30ad21e470ab8d632ac5394b4 14326425370116;95896635a240c33 73ad21e470ab8d632ac5394635a240c33 73ad21e470ab8d632ac5394635a240c33 73ad21e470ab8d632ac5394621683 56b67ee4c28276141ec0b3304672 18141bae4472ad86796e62971e1eb572 81a141bae4472ad86796e692418407 146274552726b54774534364338311d e6e579004rcd55755713420464338311d e6e579004rcd55755713ad273660792	MIPS MIPSEL Power PC SH4 ARM M68K MIPS SH4 SPARC X66 ARM M68K MIPSEL Power PC SH4 X66 ARM MIPSEL Power PC SH4 X66 ARM MIPSEL PPC SH4 ARM	2015/06 2005/06 2005/0	YES NO NO			6/13/2015 15:16
ZORRO	Bin 60 Bin 61 Bin 62 Bin 68 Bin 70 Bin 71 Bin 72 Bin 73 Bin 73 Bin 74 Bin 75 Bin 76 Bin 77 Bin 78 Bin 78 Bin 79 Bin 82 Bin 83 Bin 83 Bin 84 Bin 85 Bin 88 Bin 99	mi p s ayy,arm ayy,m68k ayy,m68k ayy,m68k ayy,sparc ayy,sp4 scanner,m68k scanner,m9s scanner,m9s scanner,m9s scanner,sh4 scanner,sh4 scanner,sh4 scanner,sh4 scanner,sh4 scanner,sh4 scanner,sh4 scanner,sh4 scanner,sh4 scanner,sh4 scanner,sh4 scanner,sh4 scanner,sh4 scanner,sh4 scanner,sh6 scanner,sh4 scanner,sh6 scann	3.369/0714 193940.35.033.003.0474/3644 16573aa67396844a.627467522053 0.d52132275420453.3f8023eb.379a.2ea frasde.0076b.022261e f 3.3086443.930b 112baee.d64abe873.6222664c53430f40 6f33aef18bc378b229eb.379a.2ea 0.7075220ba.31f992296124670 7077520ba.31f9922961256124670 707622020ba.31f9922961256124670 707622030ba.31f9922961256124670 707622030ba.31f99229612562562567239b44 4b52642308bc.3189720a52239b44 4b526423040c972612c24eef1833be32258b44 4b526425419701659-886485362440c33 73ad214470a843642642183656271aa 493cb7e947071378b13ac0439362176683 5800feec.462232286597414 tex05936721aa 493cb7e94707378b13ac043934e0f4f fc.3292Ff24c796153229b043d40339 bc5607664202322.56589741e teb572 f81a 141becd472a88766694219407 73ad21447003736b13ac043342e0f4f fc.3292Ff24c76573228b043d40339 bc5607664202322.56589741e teb572 f81a 141becd472a88766694219407 740274553246e6298633435334314 de68790bfcc.db567b5713a8d2766c79 2c514d5ac05562b5713a8d276c79 2c514d5ac05562b5713a8d276c79 2c514d5ac05562b5713a8d276c79 2c514d5ac055262559407337985460 4037078b2404232761420093395460 4037078b240423276420773854597421 1043295452254025947343574021 1043740529542025947343574021 1043740529542025947343574021 104374052954202594523459473748574021 10437405295420259452345947345574021 10437405295420259452345947345574021 10437405295420259452345947345574021 104374052954202594523455945255947345574021 104374052954202594523455945255947345574021 104374052954202594523455945255947345574021 104374552954502594523455945255947345574021 104374552954502594534557455574554525554557455455745574557455	MIPS MIPSEL Power PC SH4 ARM M68K MIPS MIPSEL Power PC SH4 SPARC x86 ARM M68K MIPS SH4 x86 ARM MIPSEL Power PC SH4 x86 ARM MIPSEL PPC SH4 X88 MIPSEL PPC	2015/06 2015/062015/06 2015/06 2015/06 2015/06 2015/062015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/062015/06 2015/0	YES NO NO			6/13/2015 15:16
ZORRO	Bin 60 Bin 61 Bin 68 Bin 69 Bin 70 Bin 71 Bin 72 Bin 72 Bin 73 Bin 74 Bin 75 Bin 76 Bin 77 Bin 78 Bin 80 Bin 81 Bin 82 Bin 82 Bin 82 Bin 82 Bin 82 Bin 82 Bin 83 Bin 84 Bin 85 Bin 88 Bin 88 Bin 88 Bin 89 Bin 99 Bin 90	mi p s ayy,arm ayy,m68k ayy,mp ayy,m68k ayy,mp ayy,ppc ayy,sh4 ayy,sparc ayy,x86 scanner,m68k scanner,m68k scanner,m68k scanner,m68k scanner,m68k scanner,m68k scanner,m68k scanner,m8 scanner,m8 scanner,sh6 a mi ppc sh armw61 i686 mips	3.3693071 (19340.32.633.0305447)844 1673aa67346844a.62746752205a3 0d521322754204533478529b.5739.26a 1725ace60768.052261 e73a306443936b 1725ace60768.052261 e73a306443936b 1725ace60748.05264525402567532142610 170775200ba3179922943532 e13056252142610 170775200ba3179922943532 e13056252142610 170752500ba3179922943532 e13056252142610 170752500ba317992294352 e1305625234 e16239593245572644-442082-3664173 13ae92a808394938811 e3711b2e94554 271700115cccd3719e706352334bd4 143524343446327c5172c2ee65ba321e 65245926264711b40504263234bd4 14352434454701695.89468358240c33 56b07ece4c28276141cc0b93b6721aa 4435cb7e4572701695.89468358240c33 56b07ece4c28276141cc0b93b6721aa 4435cb7e573229b0468342819467116693 56b07ece4c28276141cc0b93b6721aa 4435cb7e573229b0468393 161141bea404748697669697161 e16572 251445455326658974748219421907 40627d5532266ce299a33dd5382311d e6e579007ccdb56755713a827366074921907 40627d553226658b477485745274021 bc3094442326526596474748574574201 bc3094444236526596474748574574201 bc309444423652596454774853884609 4064771054650559713820458645974021 bc3094444236525964547498586460 4073705840383501ec3845255964577421 bc309444235652596454749555574021 bc3094442356525965454749555574021 bc3094442356525965454749555574021 bc3094442356525965454749555574021 bc3094442356525965454749555557452954655574201 bc3094442356525965454745555574525556454747855745255564547478557452555645547452555655457421 bc30944423565255652654547455555655547421 bc309444235652556545547455555655574201 bc30944423565255654547455555655574201 bc309444235652556555574525556555747451 bc3094545555555555555557525556455745555557525556455747621 bc3094545555555555555555555575555556555575555555	MIPS Power PC SH4 ARM M68K MIPSEL Power PC SH4 SPARC x86 ARM MIPSEL Power PC SH4 SPARC x86 ARM MIPSEL Power PC SH4 X86 ARM MIPS MIPSEL PFC SH4 ARM MIPS MI	2015/06 2015/0	YES NO NO			6/13/2015 15:16
ZORRO	Bin 60 Bin 61 Bin 62 Bin 68 Bin 70 Bin 71 Bin 72 Bin 73 Bin 74 Bin 75 Bin 76 Bin 78 Bin 78 Bin 78 Bin 78 Bin 80 Bin 81 Bin 82 Bin 83 Bin 84 Bin 85 Bin 88 Bin 99 Bin 90 Bin 91	mi p s ayy,arm ayy,m68k ayy,mp ayy,m68k ayy,sparc ayy,sp4 ayy,sp4 scanner,mps scanner,mps scanner,mps scanner,sh4 scanner,sh4 scanner,sh4 scanner,sh4 scanner,sh4 scanner,sh6 a mi ppc sh armw61 i686 mips	3.3699071 (19940.35.03.50.50.4747.1847 1673aa67.96844a.627467.622263 0d5213227.5420.453.6780.2296.379a.2ea fmeade.0078b.2228 (ef 3.30.86443.930b 112baee.d64ab.8073.822864.45340 112baee.d64ab.8073.822864.45340 112baee.d64ab.8073.822864.25841.4601.2594.163 112baee.d64ab.8073.8228664.25841.4601.2594.163 112baee.d64ab.8225864.2586732.48670 17075280ba.31199.22.903.824 46ca.893.933.857.164.45.4208c.3864.113 113a.822.8083.9432811.847.115.264564 143.5243.940.6397.081.262.8664.113 113a.822.8083.9432811.847.115.264564 143.5243.940.6397.081.262.8669.113 143.6243.940.6937.081.262.8669.114 143.5243.946.0937.081.262.8669.114 145.2643.947.0116.96.894.683.862.406.33 173.4621.447.104.804.937.081.262.8669.114 165.2639.2761.141.cob.93.95071.1aa 493.cb.7328.104.102.937.141.eb.953.95071.1aa 493.cb.7328.104.102.937.26569.7141.eb.951271.183 143.6243.8571.041.eb.9572.114.1eb.953.95071.1aa 493.cb.7328.951.041.eb.953.9571.13a.8427.866.079 12.61.463.805.3624.6525673.279b.064.863.391.114 eb.87004.cc.8525.8571.33a.8427.866.0714 14.9524.8526.8526.8526.8526.802.4147.12 40.731.1452.09.544.0257.743.5971.402.153.894.7140.21 25.61.463.805.3624.6525673.279b.0673.8391.14 eb.867004.143.250.5571.33a.8427.866.0714 25.14.05205.954.0259.073.3786.460 14.707.743.8517.463.8571.462.0453.894.674.21 25.61.463.850.7624.5526569.71.33a.8427.866.0714 25.14.05205.842.652666.962.19.407 25.14.05205.842.652666.962.19.407 25.14.05205.842.652666.962.19.407 25.14.05205.8526.85266.9627.445.2746.0774 25.14.05205.8526.85266.85266.842.742 25.14.05205.8526.85266.85266.85266.842.742 25.14.05205.8526.85266.85266.8566.8566.8566.8527.8566.972 25.14.05205.842.8566.962.19.8427.84 25.14.05205.442.8566.852666.8427.84 25.14.05205.442.8566.85666.8427.84 25.14.05205.442.8456.9667.3456.9667.7455.77455.	MIPS Power PC SH4 ARM M68K MIPS MIPS SH4 SR MIPS MIPS MIPS SH4 SPARC SH4 SPARC X86 ARM M68K MIPS SH4 X86 ARM MIPS MIPSEL PPC SH4 X86 ARM MIPSEL PPC SH4 X86 MIPS MIPS MIPS MIPS MIPS	2015/06 2015/0	YES NO NO			6/13/2015 15:16
ZORRO	Bin 60 Bin 61 Bin 69 Bin 70 Bin 71 Bin 71 Bin 72 Bin 72 Bin 73 Bin 74 Bin 75 Bin 76 Bin 77 Bin 78 Bin 79 Bin 80 Bin 81 Bin 82 Bin 82 Bin 84 Bin 85 Bin 86 Bin 87 Bin 88 Bin 89 Bin 90 Bin 91	m p s ayy.arm ayy.m68k ayy.m68k ayy.m68k ayy.pc ayy.sh4 ayy.sparc ayy.sh4 scanner.m68k scanner.m68k scanner.m68k scanner.m68k scanner.m68k scanner.m68k scanner.m8 scann	3.3899071 (1994)32.3632.0030447/3644 (1673aa67346844a.32/445022653 0.45213227542045337(8)2296.379a2ea (1726ac6076854229e17330265425533040 (1726ac6076854256425343040 (1726ac6076854256425632142670 170752608a31(9921294532)4401294613 20705232080e134(19921294532)46413 20705232080e134(19921294532)46413 2070872142942547014242082364413 13624284129342983811437114294554 136242842980348811437114294554 136242842980348811437114294554 13624234034042977611224264564234 14524434440342811437114294554 1473607115cecd3219e750455239abd4 145244354701699.8946835a240c33 5650fecc4282876141c050386471a 5650fecc4282876141c050386471a 5650fecc4282876141c050386721aa 5650fecc4282876141c050386721aa 161141bc04748697669297161269291407 406267532466cc2998a334d53a2514 16247314523246cc299873433463343911 466879061ccd55675732806463439 bcb87088610027322e56971612619407 40626753266cc29569731845374021 bcc3054442336452659675438445374021 bcc30544423364526596743384596640 47037088d303836765514534562768 56007932476293465725964627445274 30104707299633838607055562758	MIPS Power PC SH4 ARM M68K MIPSEL Power PC SH4 SPARC x86 ARM MIPSEL Power PC SH4 SPARC x86 ARM MIPSEL Power PC SH4 X66 ARM MIPS SH4 SH4 SH4	2015/06 2015/062015/06 2015/06 2015/062015/06 2015/06 2015/062015/06 2015/06 2015/062015/06 2015/06 2015/062015/06 2015/06 2015/062015/06 2015/06 2015/06 2015/062015/06 2015/06 2015/06 2015/062015/06 2015/06 2015/062005/06 2015/06 2015/06 2015/062005/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/0	YES NO NO			6/13/2015 15:16
ZORRO	Bin 60 Bin 61 Bin 62 Bin 68 Bin 70 Bin 71 Bin 72 Bin 73 Bin 74 Bin 75 Bin 76 Bin 78 Bin 78 Bin 78 Bin 78 Bin 80 Bin 81 Bin 82 Bin 83 Bin 84 Bin 85 Bin 88 Bin 99 Bin 90 Bin 92 Bin 93	mi p s ayy,arm ayy,m68k ayy,mp ayy,pp ayy,pp ayy,pp ayy,sh4 ayy,sparc ayy,sh4 scanner,mes scanner,mes scanner,mes scanner,mes scanner,sh4	3.369/0711 (1994)03:033:00304747/847 16973867196844.as2/476:022653 01d521322754204533478529b5798.2ea 112bare.db4ab.8773822664:5343040 112bare.db4ab.8773822664:5343040 112bare.db4ab.8773822664:5343040 112bare.db4ab.8773822664:5343040 112bare.db4ab.8773822664:5343040 112bare.db4ab.8773822664:5343047 112bare.db4ab.8778422662532142670 1707752080a311992293053218625284 dc3e39304571643218711b294545 13462432400514318710.25239454 1435243441639270812c2ae.825844 1435243444639270812c2ae.80451 147624152454701650.8294638a240c33 173a62144710a504264711ab003-2639454 14352454701650.8394638a240c33 173a62144710a53426459712812c2ae.80451 147624254701650.8394638a240c33 173a62144710a534342a80596689421146883 15540564634225718141c00539567128aa 433a579447107378611aad0334a0447 1668790904cc4b55752713ad02786c079 2551445ad3542645845471ab003-3839111 4668790904cc4b55755713add2786c079 2551445ad356746258b4774853774021 1bec30944423c66258b4774853774021 1bec30944423c66258b4774853774021 1bec30944423c66258b4774853774021 1bec30944423c66258b4774853774021 1bec30944423c66258b4774853774021 1bec30944423c66258b4774853774021 1bec30944423c66258b4774853774021 1bec30944423c66258b4774853774021 1bec30944423c66258b4774853774021 1bec30944423c66258b4774853774021 1bec30944423c66258b4774853774021 1bec30944423c66258b4774853774021 1bec30944423c66258b47742537660798246073986460 314bbcd07361bc46c438458b45072862786 314bbcd07361c1bc46c438458b45272678 314bbcd073c1c1b64c43855b52027271	MIPS Power PC SiH4 ARM M68K MIPS MIPS SH4 SPARC SH4 SPARC x86 ARM M68K MIPSEL Power PC SH4 x86 ARM M68K MIPSEL Power PC SH4 x86 ARM MIPSEL PPC SH4 x86 MIPSEL PPC SH4 x86 MIPS MIPS MIPS SH4 x86	2015/06 2015/062015/06 2015/06 2015/06 2015/062015/06 2015/06 2015/06 2015/062015/06 2015/06 2015/062015/06 2015/06 2015/062015/06 2015/06 2015/062015/06 2015/06 2015/062015/06 2015/06 2015/062015/06 2015/06 2015/062015/06 2015/06 2015/062015/06 2015/06 2015/062015/06 2015/06 2015/062005/06 2015/06 2015/062005/06 2015/06 2015/06 2015/062005/06 2015/06 2015/06 2015/06 2015/062005/06 2015/06 2015/06 2015/0	YES NO NO			6/13/2015 15:16
ZORRO	Bin 60 Bin 61 Bin 69 Bin 70 Bin 71 Bin 73 Bin 73 Bin 74 Bin 75 Bin 76 Bin 78 Bin 78 Bin 78 Bin 78 Bin 81 Bin 82 Bin 83 Bin 84 Bin 88 Bin 89 Bin 91 Bin 92 Bin 93	m p s ayy.arm ayy.m68k ayy.m9 ayy.m68k ayy.ppc ayy.sh4 ayy.sparc ayy.sh4 scanner.m68k scanner.m68k scanner.m68k scanner.m68k scanner.m68k scanner.m68k scanner.m84k sc	3.3893071 (19340.32.633.00.8447/3.644 1673a.6673.6647.6644.a.627467.622265.3 0.45213227.5420453.4780529.6.379.82.6 112b.ne.0614.6542.26.1673.02.6646.53.430140 1276.6607.6646.9228.646.53.430140 2076.962.32080.641973.22664.653.430140 2076.962.32080.6129.0464114.0129.0413 2076.962.32080.6124.04123.6246.0129.0413 2076.962.323080.6124.04123.624.0129.0413 2076.962.93308.6124.0412.9415.042 465.263.2080.6124.9716.042.632.6341 146.3264.3414.0363.0426.0451 147.3024.3444.0245.04514.124.0455.4 2478.07115.ce.cd321.98716.0455.239.844 145.3264.3446.04297.76112.624.64514 145.3264.3446.04297.76112.624.64514 145.3264.3446.04297.76112.624.64514 145.3264.3446.04297.76112.624.64514 145.3264.7616.7322.940.6463.0451 147.3024.7447.073.7861.134.04093.64074 165.3292.7722.471661.7328.940.8463.939.114 145.3264.7966.7322.940.6463.0451 145.3264.7966.7322.940.6463.0451 146.847.906.756.551.738.8427.986.079 125.1445.836.2462.956.971.0145.9740.21 146.879.047.645.2562.9562.636.0456.71 407.847.9564.2562.9567.633.3464.539.846.07 470.870.8642.835.807.6184.556.571.3864.2786.079 125.1445.835.4672.956.971.045.9740.21 146.879.0474.835.2462.956.971.045.9740.21 146.879.0474.835.2462.956.971.045.9740.21 147.047.945.9562.956.973.338.964.00 470.870.8642.835.967.1645.956.971.8384.00 470.870.8642.835.967.1645.956.971.8384.00 470.870.8642.835.967.1645.956.971.8384.00 470.870.8642.835.967.1645.956.971.8384.00 470.870.8642.835.967.1645.956.972.8384.00 470.870.8642.835.967.1645.956.972.8435.956.072 125.1445.835.967.0565.957.1384.2586.052.751 374.050.4473.356.256.956.973.845.956.972.8435.956.773 470.970.8442.835.967.0563.956.957.7384.956.772.270.0567.274 374.050.4473.736.256.256.957.973.845.956.773.2750.0567.758 374.050.4473.756.256.957.973.845.956.773.2750.0567.758 374.050.4476.757.257.257.257.257.257.257.257.257.257	MIPS Power PC SH4 ARM M68K MIPSEL Power PC SH4 SPARC x86 ARM MBSEL Power PC SH4 SPARC x86 ARM MIPSEL Power PC SH4 X86 ARM MIPSEL PPC SH4 X86 MIPS MIPSEL PPC SH4 X86 MIPSEL SH4 X86 MIPSEL SH4 X86 AFM	2015/06 2015/062015/06 2015/06 2015/062015/06 2015/06 2015/062015/06 2015/06 2015/062015/06 2015/06 2015/062015/06 2015/06 2015/062015/06 2015/06 2015/062015/06 2015/06 2015/062015/06 2015/06 2015/06200 2015/06 2015/06 2015/06200 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/062000 2005/06 2005/06 2	YES NO NO			
ZORRO	Bin 60 Bin 61 Bin 62 Bin 68 Bin 70 Bin 71 Bin 72 Bin 73 Bin 74 Bin 75 Bin 76 Bin 78 Bin 78 Bin 78 Bin 80 Bin 81 Bin 82 Bin 83 Bin 84 Bin 85 Bin 86 Bin 87 Bin 90 Bin 91 Bin 92 Bin 93	mi p s ayy,arm ayy,m68k ayy,m68k ayy,m68k ayy,m68k ayy,m68k ayy,m68k ayy,m68k ayy,m68k scanner,m	3.3699071 (19940.35.03.05.04747)844 (1673aa667.96844a.627467.6222653 0.45213227.5420453.41802.9b.579a.2ea freade.0078b.252e1 (7.3.086443.936b) 112bae.0478b.252e1 (7.3.086443.936b) 112bae.0478b.252e1 (7.3.086443.936b) 112bae.0478b.254645343040) 6135aefa86.78b.256642.566321.42670 70775280b.31199322903.5c143066898 405.62923096-113071162962329844 405.62923096-113071162962329844 405.62923096-113071162962329844 418.25405492454711640.3623239844 148.25405492454711640.3623239844 148.2540547164523298447116400.360651 147.6424554701656.89846838.6240633 73.a62144710a4564721640.60561 147.6424554701656.89846838.6240633 73.a62144710a436426454718400.366161 147.6424554701656.89846838.6240633 73.a62144710a436426456434364516863 56.85609861022522568697161845 439.3c1695722590.46633.38931104 64.857405405326828471840303333111 64.857405405326828471343043346747021 26.5740540530786513447235664933111 64.85740540530786513447235664933111 64.8574054053078651344723566734798456707 26.110510124933386010526734398469572 26.110510124933386010526734398469572 26.1105101249333860105267343984657275 31.44bbd.44732.68285462354625778 31.44bbd.44732.682964334362073419846577421 26.21015101249333486010527252 31.44bbd.44732.682967347984657275 31.44bbd.44732.682967347984657275 31.44bbd.44732.682967347984657275 31.44bbd.44732.68296734798457275 31.44bbd.44732.68296734798457275 31.44bbd.44732.68296734798457275 31.44bbd.44732.68296734798457275 31.44bbd.44732.68296734798457275 31.44bbd.44732.68296734798457275 31.44bbd.44732.68296734798457275 31.44bbd.44732.68296734798457275 31.44bbd.44732.68296734798457275 31.44bbd.44732.68296734798457275 31.44bbd.44732.6829673479845726275 31.44bbd.44732.68296734798457275 31.44bbd.44732.6429673467346378657275 31.44bbd.44732.64294346734657842535862776 31.44bbd.44732.64294346734657842535862776 31.44bbd.44732.64294346734657842535862776 31.44bbd.4473647545745744545455745745 31.44bbd.447364574545744545745457457457 31.44bbd.447364574545745745745745745745745745745745745	MIPS Power PC SH4 ARM M68K MIPS MIPS MIPS SH4 SPARC ×86 ARM M68K MIPS MIPSEL Power PC SH4 ×86 ARM MIPSEL Power PC SH4 ×86 ARM MIPSEL PPC SH4 ×86 MIPS SH4 ×86 ARM MIPS SH4 ×86 MIPS SH4 ×86 ARM MIPSEL SH4 ×86 ARM MIPSEL	2015/06 2015/062015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/06 2015/062015/06 2015/06 2015/062015/06 2015/06 2015/062015/06 2015/06 2015/06 2015/062015/06 2015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/06 2015/062015/06 2015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062005/06 2015/06 2015/062005/06 2015/06 2015/062005/06 2015/06 2015/062005/06 2005/06 2005/0	YES NO NO NO NO NO NO NO NO NO NO NO NO NO			
ZORRO	Bin 60 Bin 61 Bin 62 Bin 68 Bin 70 Bin 71 Bin 72 Bin 73 Bin 73 Bin 73 Bin 73 Bin 73 Bin 73 Bin 76 Bin 77 Bin 78 Bin 80 Bin 81 Bin 82 Bin 83 Bin 84 Bin 85 Bin 88 Bin 89 Bin 90 Bin 91 Bin 93 Bin 93 Bin 95 Bin 95	mi p s ayy,arm ayy,m68k ayy,m9 ayy,pc ayy,sh4 ayy,sparc ayy,sh4 scanner,m68k scanner,m88k scanne	3.38990F1 193940.35.835.005447/3844 1673aa667.46844a.624545-022653 0.d5213227.5420453.418529b.579a2aa 112bace0763b.2252e1 67.3306443936b 112bace0764b.2252e1 67.3306443936b 112bace0764b.22564d2140129brd3 20fb9b23986.6922956d256f321 12670 707/5260b.31199229403140129brd3 20fb9b23986.6922956d256f321 12670 707/5260b.31199229453.6e1 605695 10452023020 10422451701520.5239abd4 14532d334dc6927.6812.62e65baa21 te 656054622576112.6245276812.624654 14532d334dc6927.6812.62e665baa21 te 65605462.628614711bd00.38c0.6851 147-02425457011695.93968358.2406-33 5650546.428276142.624654711640.38c0.6851 147-02425457011695.93968358.2406-33 5650546.4282276141c0093.96571aa8240634 365675961c-6045755173482174063 1561141 tbec44748595665971a1 e1e5572 1511415.044246250590713340514064 4032655232466.e2996333.34053439311 405265523466.e299633.3405343931 10471814520540525967363.3405349214907 25514458.405256755713348217406271 2651944423.36452567557134857460.79 25514458.405256755713485740052786 261079112.6464263256756713485740271 bec30944423.3645256756713485740271 bec30944423.3645256752384054272 2514458.405256755713485740052786278 25104781.1542052567571348574052786 25104781.1542052781534574052781 25214458.405256753346452781528050757384540 25104781.15420542557314652785134574052781 3645755851414337685854743537405278134 36567595153454255278134357538194	MIPS Power PC SH4 ARM M68K MIPSEL Power PC SH4 SPARC x86 ARM M68K MIPSEL Power PC SH4 SPARC x86 ARM MIPSEL Power PC SH4 x86 ARM MIPSEL PPC SH4 x86 MIPS SH4 x86 MIPSEL SH4 x86 MIPSEL SH4 x86 ARM x86 ARM MIPSEL SH4 x86 ARM MIPSEL SH4 X86 ARM MIPSEL SH4 X86	2015/06 2015/062015/06 2015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062005/06 2015/062005/06 2015/06 2015/062005/06 2015/06 2015/062005/06 2015/06 2015/062005/06 2005/06 2005/0	YES NO NO			
ZORRO	Bin 60 Bin 61 Bin 68 Bin 69 Bin 70 Bin 71 Bin 72 Bin 73 Bin 74 Bin 75 Bin 76 Bin 77 Bin 78 Bin 79 Bin 80 Bin 81 Bin 82 Bin 82 Bin 84 Bin 85 Bin 88 Bin 89 Bin 99 Bin 91 Bin 92 Bin 94 Bin 95 Bin 96 Bin 97	mi p s ayy.am ayy.m68k ayy.mp ayy.m68k ayy.mp ayy.ppc ayy.sh4 ayy.sparc ayy.x86 scanner.m9k scanner.m9k scanner.m9k scanner.m8	3.369/0711 (1994)03:033:03003471/3644 1673aa67346844ao22445702263 0.d521322754204533418529b.579a2ea freadec0078b.522e1 e733ab6443936b 112baec61443936b 112baec61443936b 213baec6147b.22364c53430140 6735aefa8c778b.2294c8144012945d3 2050b9.23866eb.225564c256673214670 70775200b321945294048144012945d3 2050b9.23866b.2255642566732146270 2050b9.238659402586724442086368235484 efca.8986394638511e.3711b2e945b4 747780115cced3219e70a52239abd4 14352043945097c812c2ee65baa21e 2050c24302000000000000000000000000000000000	MIPSEL Power PC SH4 ARM M68K MIPSEL Power PC SH4 SPARC x86 ARM M68K MIPSEL Power PC SH4 SPARC x86 ARM MIPSEL Power PC SH4 X86 ARM MIPSEL PPC SH4 ARM MIPSEL PPC SH4 ARM MIPSEL SH4 ARM X86 ARM X86 ARM MIPSEL SH4 X86 ARM MIPSEL MIPSEL MIPSEL MIPSEL PPC	2015/06 2015/062015/06 2015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062005/06 2015/062005/06 2015/062005/06 2015/06 2015/062005/06 2015/062005/06 2005/06 2005/06 2005/0	YES NO NO			
ZORRO	Bin 60 Bin 61 Bin 62 Bin 63 Bin 70 Bin 71 Bin 72 Bin 73 Bin 76 Bin 77 Bin 78 Bin 80 Bin 81 Bin 82 Bin 83 Bin 84 Bin 85 Bin 86 Bin 87 Bin 80 Bin 81 Bin 83 Bin 80 Bin 81 Bin 83 Bin 90 Bin 91 Bin 92 Bin 93 Bin 94 Bin 95 Bin 96 Bin 97 Bin 98	mi p s ayy,arm ayy,m68k ayy,m68k ayy,m68k ayy,sparc ayy,sh4 ayy,sparc ayy,sh4 scanner,arm scanner,m68k scanner,m68k scanner,m68k scanner,m68k scanner,m68k scanner,sh4 scanner,sh4 scanner,sh4 scanner,sh4 scanner,sh4 sh4 armv61 ii686 mipsel sh4 armv61 ii686,64 armm mipselm mipselm sh4 armm sh4 armm	3.38990F1 193940.35.03.50.05447.3844 1673a.6673.4673.46844.as.24F6.22265.3 0.45213227.5420453.478529b.579.82.as 17.82.nsc0454.as 17.82.nsc0454.as 17.82.nsc0454.as 17.82.nsc0454.as 17.82.nsc0454.as 17.82.nsc0454.as 17.82.nsc0454.as 17.82.852.452.452.452.452.452.452.452.452.452.4	MIPS Power PC SH4 ARM M68K MIPSEL Power PC SH4 SPARC x86 ARM M68K MIPSEL Power PC SH4 MBS MIPSEL Power PC SH4 x86 ARM MIPSEL PPC SH4 ARM x86 MIPS SH4 ARM x86 MIPSEL SH4 X86 AFM MIPSEL SH4	2015/06 2015/062015/06 2015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062005/06 2015/062005/06 2015/06 2015/062005/06 2015/062005/06 2005/06 2005/06 2005/06 2005/0	YES NO NO			
ZORRO	Bin 60 Bin 61 Bin 68 Bin 69 Bin 70 Bin 71 Bin 72 Bin 73 Bin 74 Bin 75 Bin 76 Bin 77 Bin 78 Bin 79 Bin 80 Bin 81 Bin 82 Bin 82 Bin 82 Bin 84 Bin 85 Bin 86 Bin 87 Bin 90 Bin 91 Bin 92 Bin 93 Bin 94 Bin 95 Bin 96 Bin 97 Bin 98 Bin 98 Bin 97 Bin 98 Bin 99 Bi	mi p s ayy,am ayy,m68k ayy,mp ayy,m68k ayy,mp ayy,ppc ayy,sh4 ayy,sparc ayy,sh4 scanner.m68k scanner.m68k scanner.m68k scanner.m68k scanner.m68k scanner.m68k scanner.m68k scanner.m68k scanner.m68k scanner.m68k scanner.st	3.3693071 (19340.35.03.005447)844 (1673aa67346844a.3244570.22653 0.4521322754204533418529b.5739.26a 112baced54ab.2251e (7.33084443936b 112baced54ab.2251e (7.33084443936b 112baced54ab.2251e (7.33084443936b 112baced54ab.2251e (7.3308443936b 112baced54ab.2251e (7.3308443936b 112baced54ab.2251e (7.3308443936b 112baced54ab.2251e (7.3308443936b 112baced54ab.2251e (7.3308443936b 112baced54ab.2251e (7.330842521e) 13ae92a808349438811e 3711b2e3654 14a524344163362811e 3711b2e3654 14a5243446327c812c22ee65baa21e 14a5243446327c812c22ee65baa21e 14a5244547011695.8806835a240c33 13ae424670471695.8806835a240c33 13ae424670471695.8806835a240c33 13a2421e 470bac4d32acb39421f683 35b0fece4c282276141cb053b3671aa 4433cb7486170675322b064857385 14a5242456701695.8806835a240c33 12a421e 470bac4d32acb39671683 35b0fece4c282276141cb053b3671aa 4433cb74861702675322b064857385 1514161b264742652761732b303464393 1524142645470265b8477485174821 15251445a352665b8477485174821 1525144543526265b8474784577421 1525144543532665b8474784577421 1525144545352665b847478457457421 1525144545352665b847484555b22761 14270471152652665b847484555b22761 14267431b45267452596454734555577801 1452444235612656732845456742184 2671071151243232467505658773281 112b6772951328545658747021 152514455352665b847484555b22761 152514455352665585747201 1525145535352665585778021 1525145535352665585778021 1525145535352665585778021 1525145535352665585778021 1525145535352665585778021 1525145535352665585778021 1525145535352665585778021 15251455353565555778021 1525145535352665585778021 15251455353574525596547474557864374021 15251455555755732596585778021 15251455555755732596585778021 1525145555575573864605585778021 1525145555575578644744565555778021 1525758575857585758575857585786474474865 15257587578575875874447448575878444744865 152575875874447448575878444744865 152575878447448575878444744865 152575878447448575878444744865 15257587844744857587844744865 15257587844744857587844744865 15257587844744850578444744865 15257587844744865 154575	MIPS Power PC SH4 ARM M68K MIPS MIPS MIPS SH4 SPARC SH SPARC X66 ARM MIPSEL Power PC SH4 X86 ARM MIPSEL Power PC SH4 X86 ARM MIPS MIPSEL PPC SH4 ARM x86 ARM MIPSEL SH4 X86 ARM X86 ARM MIPSEL SH4 X86 ARM MIPSEL MIPS ARM MIPS ARM ARM ARM MIPS ARM	2015/06 2015/062015/06 2015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062005/06 2015/062015/06 2015/062005/06 2015/062005/06 2005/06 2005/06 2005/0	YES NO NO	10 / 57	6/22/2015 21:12	6/13/2015 15:16
ZORRO	Bin 60 Bin 61 Bin 62 Bin 63 Bin 70 Bin 71 Bin 72 Bin 73 Bin 73 Bin 73 Bin 73 Bin 73 Bin 76 Bin 77 Bin 78 Bin 78 Bin 80 Bin 81 Bin 82 Bin 83 Bin 84 Bin 85 Bin 88 Bin 90 Bin 91 Bin 93 Bin 95 Bin 97 Bin 98 Bin 97 Bin 98 Bin 97 Bin 98 Bin 97 Bin 98 Bin 99 Bin 90	mi p s ayy,arm ayy,m68k ayy,m68k ayy,m68k ayy,sparc ayy,sparc ayy,sparc ayy,sparc ayy,sparc scanner,m68k scanner,m68k scanner,m68k scanner,m68k scanner,sh4 scanner,sh4 scanner,sh4 scanner,sh4 scanner,sh4 scanner,sh4 sh4 armm61 i686,64 armm mipselm mipselm mipselm mipselm mipselm mipselm mipselm mipselm mipselm mipselm	3.38990F1 193940.35.835.005447.844 1673aa667.84684.as24545-02265.3 0d5213227.5202453.348529b.579a2ea freade.co078a.0522ea 17.33ab64338bb 112bace044ab6773e2264453.430140 20f53acf8.267482-268461354.030140 20f53acf8.267482-268461354.031246 20f53acf8.267482-26846134.0129k1d3 20f5.9b2.3986.05228564256f632142670 7077520803.11931229405340 20f53acf8.267482-2648614.0129k1d3 20f5.9b2.3986.05228564256f632142670 20f53acf8.267482045314.0129k1d3 20f5.9b2.3986.05228564256f632142670 20f5.25208061.032241143366.252684 145.244543701459.258048114.371142.945544 145.244543701459.258048114.371142.945544 145.24454701459.2580481342412.945544 145.244547071459.25804834240-23328.9464 246.3278967.227978613.34003420.04551 15.147.0424547071659.25990.048646039 16.252276242.7965732299.048646039 16.252276242.7965732299.048646039 16.252876242.7965732299.048646039 16.252876242.7965732299.048464039 16.252876242.7965732299.048464039 16.252876242.7965732299.048464039 16.252876242.796573299.048464039 19.25144520565755713.342774021 19.2514452056575713.34275402.71 10.25840105101.265420259.073.34986460 24.700.700.84383.840161.63433.8559140 14.702.700.84383.840161.63433.855914 14.702.700.84383.840161.26343.8455942780 24.5145520.842589673.34974202710 10.25840105101.36147.43633592-26124 20.115101.ac6647.23631.940146577 14.857.558.1640643.9455592781 34.2104711.26657.23843.940195052781 34.2104711.26657.23843.94019502781 34.2104711.26657.23843.94019502781 34.2104711.26657.23843.94019502781 34.2104711.26657.23843.94019502781 34.2104711.26657.23843.940195052781 34.2104711.26657.23843.940195052781 34.2104711.26657.23843.940195052781 34.2104711.26657.23843.940195052781 34.2104711.26657.23843.940195052781 34.2104711.26657.23843.940194577 34.2104711.26657.23843.940194577 34.2104711.26677.23843.9401946577 34.2104711.26677.23843.9401946577 34.2104712.26679.26679.26794743.940104782 34.2104712.26679.2679474748577572.264757474857772.21047781 34.210578.2447428424708407422 34.210578.24474784577422.26687975.77 34.2104	MIPS MIPSEL Power PC SH4 ARM M68K MIPSEL Power PC SH4 SPARC SPARC SPARC MIPSEL Power PC SH4 MIPSEL Power PC SH4 X66 ARM MIPSEL PPC SH4 ARM X66 MIPS SH4 ARM X66 MIPSEL SH4 ARM MIPSEL MIPS SH4 ARM V98	2015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062000 2015/06 2015/062000 20000000000000000000000000000000	YES NO NO	10 / 57	6/22/2015 21:12	6/13/2015 15:16
ZORRO GAYFGT *.sh	Bin 60 Bin 61 Bin 69 Bin 70 Bin 71 Bin 72 Bin 73 Bin 74 Bin 75 Bin 76 Bin 77 Bin 78 Bin 78 Bin 79 Bin 80 Bin 81 Bin 82 Bin 82 Bin 84 Bin 85 Bin 86 Bin 87 Bin 90 Bin 91 Bin 92 Bin 93 Bin 94 Bin 95 Bin 96 Bin 97 Bin 98 Bi	mi p s ayy.arm ayy.m68k ayy.m9 ayy.pc ayy.sh4 ayy.sparc ayy.sh4 scanner.m68k scanner.m68k scanner.m68k scanner.m68k scanner.m68k scanner.m68k scanner.m68k scanner.m68k scanner.m68k scanner.m68k scanner.m68k scanner.m68k scanner.m68k scanner.m68k scanner.m68k scanner.s86 a mi ppc sh4 x86.64 armm mipsel sh4 x86.64 armm mipsel sh4 x86.64 armm mipsel sh4 x86.64 armm mipsel sh4 sh4 x86.64 armm mipsel sh4 sh4 x86.64 armm mipsel sh4 sh4 x86.64 armm mipsel sh5 sh5 sh5 sh5 sh5 sh5 sh5 sh5 sh5 sh5	3.3499071 (1994)03:033:005447)3644 (1673aa67346844a.02/445622053 0.4521322754204533(185296)379a2ea (1726ae007805220 e1 73308443936b 112bae0614ab9220 e1 73308443936b 112bae0614ab9220 e1 73308443936b 112bae064473622644533(2014) 6735aefa8c178b2294ad814e01294fd3 2015b23986e522566425663214870 1070752008a31(19912294)36263214870 1070752008a31(19912294)36263214870 107075200831(19912294)362632394b4 146324394369276812c27ee685a2168 147070115cced331197504552394b4 1485244394469276812c27ee685a21e 626399393657C4444c4208c3664173 1362e6453002c264711b4003a260451 147024454701695.9806835a240c33 56b0fece4c28276141cc0b93b6721aaa 443ac1a4940434d2ac2b39f4216683 56b0fece4c28276141cc0b93b6721aaa 443ac1a494070378613aad033ac04511 161341bead47486976696921407 4062rd5532266c299en33d4038931401 4062rd5532266c299en33d403893141 4062rd5532266c299en33d4038921407 4062rd5532266c299en33d45389314 4700708d403a3b611692784557420 16141b26444292689613642784 1011b4672334446355bb2027e1 251445ad5542659647485574201 bec30944423c628567284044827 2610071b124933ac476bb187662784 301b46727845134965696973814 40703708d40338c916763343849660 2674010510124923ac46bb187662784 301b4672786113ad2786601786 2610071b124933ac46bb187662784 301b46727841130376855781414b57602 26100562758 344bb04423c6289615a5785414b57602 26100562758 344bb0478114303768557824414207660562758 344bb0478114303768557854144b76502 345b54645381437b565847444337685847784 261007161143376855785414b57602 26100716114337685578641442074486 2610071645738194 2610476457381143778651782426800567788194 26104764573847784 26104764573447774847784 2610476457444774847784 261047645758447774847784	MIPS Power PC SH4 ARM M68K MIPSEL Power PC SH4 SPARC x86 ARM MIPSEL Power PC SH4 SPARC x86 ARM MIPSEL Power PC SH4 X86 ARM MIPS MIPSEL PPC SH4 ARM x86 MIPS MIPSEL SH4 x86 ARM MIPSEL SH4 x86 ARM MIPS MIPSEL SH4 x86 ARM MIPS ARM ARM MIPS SH4 X86 ARM MIPS	2015/06 2015/062015/06 2015/062015/06 2015/06 2015/062015/06 2015/06 2015/062015/06 2015/062015/06 2015/062005/06 2015/0	YES NO NO	10 / 57	6/22/2015 21:12	6/13/2015 15:16
ZORRO GAYFGT *.sh	Bin 60 Bin 61 Bin 62 Bin 63 Bin 70 Bin 71 Bin 72 Bin 73 Bin 76 Bin 77 Bin 78 Bin 78 Bin 81 Bin 82 Bin 83 Bin 84 Bin 85 Bin 86 Bin 91 Bin 92 Bin 93 Bin 94 Bin 95 Bin 97 Bin 98 Bin 97 Bin 98 Bin 97 Bin 98 Bin 99 Bin 100 Bin 101 Bin 100	mi p s ayy,arm ayy,m68k ayy,m68k ayy,m68k ayy,sparc ayy,sparc ayy,sparc ayy,sparc scanner,mps scanner,mps scanner,mps scanner,mps scanner,sh4 scanner,sh4 scanner,sh4 scanner,sh4 scanner,sh4 scanner,sh4 sh4 armw61 i686 mips sh4 ash6,64 armm mipselm mipselm mipselm mipselm mipselm mipselm shm mipselm mi	3.389071 193940.35.835.0054473844 1673aa673.676844a.632445-022653 0.d52132275.202453.318529b.379a2aa 112bace0454.2025a173.80264453.300140 12bace0454.20246134.0129413 20fb.9b23986.92285642564533.00140 20fb.9b23986.92285642564532102670 7077526043119312290.30261129413 20fb.9b23986.92285642564532102670 707752693831.93271429413 20fb.9b23986.92285642564532102670 707752693831.9327142.94514 20fb.9b23986.92285642564532142670 20f527203026129413 20fb.9b23986.92285642564532142670 20f52720302632831.13271142.945144 143244344469307.76112.2648544 143244344469307.76112.2648544 143244547011659-0348613634240-03 2560454302.262864711b.db0.38420.651 15147-0424557016159-03486336240-03 25604543027366113.2604934216683 2560766-c4282276141c.0b939.6721aa 4363.179497773786113.2604934.04014 ffc.3229247.2427967522939.043846893 161414bac4423486966.694219407 4062165322466.e2998-0333405.439311 db63044423486966.694219407 406216532466.e2998-0333405.439311 db630444234679657533406.073374021 40731b4520954502598-073.3986460 2710971b12403.034465019662784 4700.706343434010550557313.34275480.799 2514435034142034696647340547420 2410911b12403.034465019662784 4700.706343434010550558774021 106247540510555133482762784 4700.70634343401156053447420454774853774021 47731b4520954502598-073.33474021 4700.7084343401055055877334144054774853774021 47731b4520954502598-073.3347380174021 4747515461249545015473434244744447444444444444444444444444	MIPSEL Power PC SH4 ARM M68K MIPSEL Power PC SH4 SPARC SPARC SH4 SPARC SH4 SPARC SH4 SPARC SH4 MIPSEL Power PC SH4 ARM MIPSEL SPAC SH4 ARM MIPSEL SH4 ARM MIPS SH4 ARM MIPSEL SH4 ARM MIPSEL MIPS PFC SH4 ARM x88 MIPS SH4 ARM	2015/06 2015/062015/06 2015/062015/06 2015/06 2015/062015/06 2015/06 2015/062015/06 2015/06 2015/062015/06 2015/062015/06 2015/0	YES NO NO	10 / 57	6/22/2015 21:12 8/22/2015 21:12	6/13/2015 15:16
ZORRO GAYFGT *.sh	Bin 60 Bin 61 Bin 68 Bin 70 Bin 71 Bin 72 Bin 73 Bin 73 Bin 74 Bin 75 Bin 76 Bin 78 Bin 78 Bin 78 Bin 78 Bin 81 Bin 82 Bin 83 Bin 84 Bin 88 Bin 99 Bin 90 Bin 91 Bin 92 Bin 93 Bin 94 Bin 99 Bin 100 Bin 101 Bin 101	mi p s ayy.arm ayy.m68k ayy.m9 ayy.pc ayy.sh4 ayy.sparc ayy.sh4 scanner.m68k scanner.m8k scanner.m68k scanner	3.3893071 (19340.32.633.0030447)844 1673a.6673.4684.362445.02265.3 0.45213227.5420453.4780.298.579.82.6 112b.nec.0643.652.208.673.02644.336.6 112b.nec.0643.652.208.673.02644.336.6 112b.nec.0643.0256.4256.632.12670.7 170752604.31199.1229.035.212670.7 170752604.31199.1229.035.212670.7 170752604.31199.1229.035.212670.2 160.252.32080-1129.2524.2529.4 160.2529.3296.1229.4212.4228.2529.4 160.2529.3296.1229.4212.4228.2539.4 145.224.3414.6326.4311.4326.4556.4228.4 145.224.3444.6297.1631.62.269.4614.3 146.224.3446.4271.6312.62.266.4615.3 147.024.455.701.699.8968.836.2410.635 154.074.245.4701.699.8968.836.240.635 154.074.245.4701.699.8968.836.240.635 154.074.245.4701.699.89683.8240.635 154.074.245.4701.699.89683.8240.635 154.074.245.4701.699.89683.8240.635 154.074.245.4701.699.89683.8240.635 154.074.245.4701.699.89683.8240.635 154.074.245.4701.699.89683.8240.635 154.074.245.4701.699.89683.8240.635 154.074.245.4701.699.89683.8240.635 154.074.245.4701.699.89683.8240.635 164.141.bc.ed.443.245.059671.418.645.645.645 164.743.045.655.571.389.643.645.657 164.875.655.571.389.643.645.657 164.875.655.571.389.647.645.671.93 162.674.4453.362.659.657.329.80.646.452 164.743.145.2695.455.259.667.239.80.467.743 174.718.145.209.454.455.557.13.895.4450 174.718.144.230.245.455.573.896.440 174.718.145.209.245.455.573.896.440 174.718.145.209.2454.273.4455.586.275.1453.375.319.44 164.843.350.671.633.755.319.4455.557.319.44 164.843.265.255.22.8600.562.753 174.835.262.896.1547.3435.2455.22.3500.275.1 174.835.252.835.2455.255.235.235.2455.255.235.2455.255.235.2455.255.235.2455.255.255.235.2455.255.2455.255.255.2455.255.255.255	MIPS Power PC SH4 ARM M68K MIPSEL Power PC SH4 SPARC x86 ARM MIPSEL Power PC SH4 SPARC x86 ARM MIPSEL Power PC SH4 X66 ARM MIPS SH4 X86 ARM MIPS PFC SH4 X86 MIPS PFC SH4 X86 MIPS PFC	2015/06 2015/062015/06 2015/06 2015/062015/06 2015/06 2015/062015/06 2015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/0	YES NO NO	10 / 57	6/22/2015 2112 6/22/2015 2113 6/22/2015 21 13	6/13/2015 15:16
ZORRO GAYFGT *.sh	Bin 60 Bin 61 Bin 62 Bin 63 Bin 70 Bin 71 Bin 72 Bin 73 Bin 73 Bin 74 Bin 75 Bin 76 Bin 78 Bin 78 Bin 78 Bin 78 Bin 78 Bin 80 Bin 81 Bin 82 Bin 83 Bin 84 Bin 85 Bin 88 Bin 90 Bin 91 Bin 92 Bin 93 Bin 95 Bin 96 Bin 97 Bin 98 Bin 99 Bin 100 Bin 101 Bin 102 Bin 102	mi p s ayy,arm ayy,m68k ayy,m9 ayy,m9 ayy,m9 ayy,m9 scanner,m9 sca	3.369/0711 (193940.35.03.50.05.94.07.18.47 16573a.667.94684.94.62.2445.02.25.63 0.452.13.22.75.42.045.33.416.22.96.37.98.26.a 17.25.86.47.86.25.26.17.33.04.84.93.95.0 17.25.86.47.86.25.26.17.33.04.84.93.95.0 17.25.86.47.86.25.26.17.86.25.24.047.0 17.07.15.20.80.31.19.93.22.94.05.21.047.0 17.07.15.20.80.31.19.93.22.94.05.21.047.0 17.07.15.20.80.31.19.93.22.94.05.22.05.0 13.86.92.86.92.85.66.22.65.65.23.046.0 13.86.92.86.92.85.66.25.85.65.23.046.0 14.05.20.80.94.19.93.22.94.05.23.94.04 14.85.20.43.24.94.11.83.65.22.85.04 14.85.20.43.24.04.11.83.65.23.94.04 14.85.20.43.24.04.19.85.20.85.04 14.85.20.43.24.04.05.85.23.94.04 14.85.20.43.24.04.05.05.05.23.94.04 14.85.20.43.24.05.05.05.23.94.04 14.85.20.43.24.05.05.05.05.05.05.05.05.05.05.05.05.05.	MIPSEL Power PC SH4 ARM M68K MIPSEL Power PC SH4 SPARC x86 ARM M68K MIPSEL Power PC SH4 SPARC x86 ARM MIPSEL Power PC SH4 X86 ARM MIPSEL PPC SH4 X86 ARM MIPSEL SH4 X86 ARM X86 ARM X86 ARM X86 ARM X86 ARM MIPSEL MIPS SH4 X86 MIPS PPC SH4 ARM MIPS SH4	2015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062015/0	YES NO NO	10 / 57	6/22/2015 21:12 6/22/2015 21:12 6/22/2015 21:13 6/22/2015 21:13	6/13/2015 15:16
ZORRO GAYFGT *.sh	Bin 60 Bin 61 Bin 68 Bin 70 Bin 71 Bin 72 Bin 73 Bin 74 Bin 75 Bin 76 Bin 77 Bin 78 Bin 80 Bin 81 Bin 82 Bin 83 Bin 84 Bin 85 Bin 86 Bin 91 Bin 92 Bin 93 Bin 94 Bin 95 Bin 96 Bin 97 Bin 98 Bin 98 Bin 99 Bin 100 Bin 101 Bin 102 Bin 103 Bin 103 Bin 103	mi p s ayy.arm ayy.m68k ayy.m9 ayy.pc ayy.sh4 ayy.sparc ayy.sh4 ayy.sparc ayy.sh4 scanner.m68k s	3.3499071 (19394)32.633.0030447/3644 1673a.6673.04673.46844-a62445-62265- 0.45213227.5420453.418529b.579.26a 112b.nec.0643.62226.173.304643.936b 112b.nec.0643.05226.173.052645.533.03040 2076.962.9396.692295642.567321.26670 70775260b.3119932294.0521.0297d 2076.962.9396.692295642.567321.26670 70775260b.3119932294.052.61366.6588 405.622302006.10322.441183356.21364.553 405.622302006.10322.4311.8373.162.94534 146.3243046.0527.0512.62.466.458 147.262453.0701.0159.854811.63711.162.94534 147.3624.3344.6297.7613.62.466.458 246.639.936.264711.b60.362.406.51 147.3624.454.701169.95486435.8240.63 569.076.ec.492.8227.6112.62.466.83 569.076.ec.492.8227.6112.62.466.83 569.076.ec.492.8227.6141.c0.093.96721.883 569.076.ec.492.8227.6141.c0.093.96721.883 569.076.ec.492.8227.6141.26.093.96721.883 569.076.ec.492.8227.6141.26.093.96721.883 569.076.ec.495.8057.513.3427.9466.079 2.514.456.455.25675.573.33427.9466.079 2.514.456.455.25675.573.33427.9466.079 2.514.456.455.2565.256.971.81.457.1426.079 2.514.456.455.2565.573.33427.802.864.074 4700.708.4423.2364.556.557.573.3457.8456.079 2.514.456.356.256.556.573.229.0466.278 4031.0476.1249.652.867.056.971.834.5774.802.771 2.514.456.455.856.256.972.78 3.443.0457.856.056.957.573.334.957.573.194 2.514.453.2465.256.256.0573.234.957.531.94 2.514.453.2465.256.265.265.267.533.956.278 3.443.0457.856.256.256.278.855.278 3.443.0457.856.256.256.278.855.278 3.4442.266.2651.557.573.334.2757.531.94 3.4442.266.2651.567.573.334.255.252.266.0527.81 3.443.544.232.6455.557.531.945.278.319.4 3.4442.266.2651.567.278.319.4 3.4442.266.2651.567.278.319.4 3.4442.266.2651.567.278.319.4 3.4442.266.2651.567.278.319.4 3.4442.266.2651.567.278.319.4 3.4442.266.2651.567.278.319.4 3.4454.437.357.557.373.347.257.319.4 3.4454.437.357.557.373.347.257.319.4 3.4654.437.357.557.373.347.257.373.94 3.4654.437.4553.276.262.263.2660.857.373.97 3.4654.437.4553.276.262.263.2663.373.05 3.4654.433.437.4537.357.357.373.94 3.4654.433.437.4537.357.373.94 3.4654.437.4537.357.373.94 3.4654	MIPS Power PC SH4 ARM M68K MIPSEL Power PC SH4 SPARC x86 ARM MBSEL Power PC SH4 SPARC x86 ARM MIPSEL Power PC SH4 X86 MIPSEL PPC SH4 X86 MIPS MIPSEL SH4 X86 MIPS SH4 X86 MIPSEL SH4 X86 MIPS SH4 X86 ARM MIPSEL SH4 X86 MIPS SH4 X86 MIPS SH4 X86 MIPS MIPS	2015/06 2015/062015/06 2015/06 2015/062015/06 2015/06 2015/062015/06 2015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/0	YES NO NO	10 / 57	6/22/2015 21:12 6/22/2015 21:12 6/22/2015 21:13 6/22/2015 21:12	6/13/2015 15:16 6/22/2015 21:12 6/22/2015 21:12 6/22/2015 21:12
ZORRO GAYFGT *sh	Bin 60 Bin 61 Bin 62 Bin 63 Bin 70 Bin 71 Bin 72 Bin 73 Bin 73 Bin 74 Bin 75 Bin 76 Bin 77 Bin 78 Bin 78 Bin 78 Bin 78 Bin 80 Bin 81 Bin 82 Bin 83 Bin 84 Bin 85 Bin 88 Bin 99 Bin 90 Bin 91 Bin 92 Bin 93 Bin 95 Bin 96 Bin 97 Bin 98 Bin 99 Bin 100 Bin 101 Bin 102 Bin 103	mi p s ayy,m68k ayy,m68k ayy,m68k ayy,mp ayy,pp ayy,pp ayy,pp ayy,sh4 ayy,sparc eyy,sh6 scanner,mps scanner,mps scanner,mps scanner,mps scanner,mp scanner,ms scanner,mp scanner,sh4 scann	3.369/0711 (1994)03:033:03054471844 (1673aa6719684)aa627467522053 01d521322754204533(18529b57)9a2ea (172beed60768522261 e73ab6443936b 112beed694ab6733e2264c53430140 6735aefa8c778b229e1733ab678324470 127057250ba3119932294353e14001282 1260b95238665922566425663214670 70775200ba311993229435ae1406689 405a292300e1 ad22441183362823644 efca896393a657Ca444c4208c3664153 13ae92a808394058811e3711b2e945b4 747780115cced3719e70a55239abd4 143520434463927c812c2ee65baa21e 60c38930e57Ca44c4208c3664153 13ae2280829405811e3711b2e945b4 74780115cced3719e70a55239abd4 143520434463927c812c2ee65baa21e 60c39590c204571b104058406836z40c33 13ad21e470ab43642ac5964853ac40c33 13ad21e470ab43642ac596971e1eb582 56b07ece4228276141ec0b3304671 66c329762c245697322b0466353 14c204553205462698471ab043ac40633 15cb87069610207322c5669971a1eb582 56b07ece428276141ec0b3304571 1a6287704715c3338697056589731e1eb576 251445ab4526954625986473a508453 11626745532528b44774354567092 251445454570425586973a1984650 470708643633401cc364533abe9657 251445ab452658457421 bec309444235658454145677421 bec30944423555875414b57602 25144545453742558645774321 bec30944423535658451445767021 bec30944423535658451445767021 bec30944423535658454145677421 bec3094442353565845474258 0546492eed81664723425457031 054675329746690932427040174255 0546492546913724555957732594046577821 165677525946690932427040774255 16574745756690932427040774255 054692eed816578571421 15675742595690932474203746575259 16575745577259 165757457574577257574577221 1657757457757457721 1657757457574577221 1657757457574577221 16577574577574577221 1657757457757457722175633389690055758 37440504720590597325757421 1657757457757457722175633386775753199 1654755259728797722175633389690052758 374405047205909795555377722177645737457574571 1654757537467777277651745777727765177657474774656 1674745590590979785555777726451 16747455905909795555577776457776451 16747455905909795555577776457776451 1565656253296262474675592962424	MIPSEL Power PC SH4 ARM M68K MIPSEL Power PC SH4 SPARC x86 ARM M68K MIPSEL Power PC SH4 SPARC x86 ARM MIPSEL Power PC SH4 X86 ARM MIPSEL PPC SH4 ARM X86 MIPSEL SH4 ARM X86 ARM SH4 SH4 ARM X86 ARM MIPSEL MIPS ARM ARM ARM ARM ARM ARM ARM ARM ARM ARM </td <td>2015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062015/062015/06 2015/062015/0</td> <td>YES NO NO</td> <td>10 / 57</td> <td>6/22/2015 21.12 6/22/2015 21.13 6/22/2015 21.12 6/22/2015 21.12</td> <td>6/13/2015 15:16 6/22/2015 21:12 6/22/2015 21:12 6/22/2015 21:12 6/22/2015 21:12</td>	2015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062015/06 2015/062015/062015/06 2015/062015/0	YES NO NO	10 / 57	6/22/2015 21.12 6/22/2015 21.13 6/22/2015 21.12 6/22/2015 21.12	6/13/2015 15:16 6/22/2015 21:12 6/22/2015 21:12 6/22/2015 21:12 6/22/2015 21:12

$\label{eq:table} Table \ A{\cdot}1 \quad \mbox{Malware binary files captured by IoTPOT}.$



Yin Minn Pa Pa received her B.E. in Information Technology in 2006 from Mandalay Technological University, Myanmar and M.Phil. in Infrastructure Management in 2013 from Yokohama National University, Japan. She is currently Ph.D. candidate of Information Media and Environment Science Course of Graduate School

of Environment and Information Sciences, Yokohama National University. She is going to finish her Ph.D. in March 2016. Her research interest is network security. She received best paper award in Asia-JCIS, 2013 and best technical report award of the year by Information and Communication System Security (ICSS) 2013, Japan.



Shogo Suzuki is currently second year Master student of Information Media and Environment Science Course of Graduate School of Environment and Information Sciences, Yokohama National University. He is going to finish his M.E. in Computer Engineering in March 2016. His research interest is network security.



Takahiro Kasama received his B.E. and M.E. and Ph.D. degrees in Computer Engineering from Yokohama National University in 2009 and 2011, 2014, respectively. He is currently a researcher at the National Institute of Information and Communications Technology, Japan. His research interest covers a wide area of net-

work security including network monitoring and malware analysis. He received the Best Paper Award at the Computer Security Symposium 2010 (CSS2010), and the IPSJ Yamashita SIG Research Award in 2011.



Katsunari Yoshioka received his B.E., M.E. and Ph.D. degrees in Computer Engineering from Yokohama National University in 2000, 2002, 2005, respectively. From 2005 to 2007, he was a Researcher at the National Institute of Information and Communications Technology, Japan. Currently, he is an Associate Professor

for Division of Social Environment and Informatics, Graduate School of Environment and Information Sciences, Yokohama National University. His research interest covers a wide range of information security, including malware analysis, network monitoring, intrusion detection, and information hiding. He was awarded 2009 Prizes for Science and Technology by The Commendation for Science and Technology by the Minister of Education, Culture, Sports, Science and Technology.



Tsutomu Matsumoto is a professor of the Graduate School of Environment and Information Sciences, Yokohama National University and directing the Research Unit for Information and Physical Security at the Institute of Advanced Sciences. He received his Doctor of Engineering from the University of Tokyo in

1986. Starting from Cryptography in the early 80's, he has opened up the field of security measuring for logical and physical security mechanisms. Currently he is interested in research and education of Embedded Security Systems such as Smartcards, Network Appliances, Mobile Terminals, In-vehicle Networks, Biometrics, and Artifact-metrics. He is serving as a program officer of the JSPS Research Center for Science Systems, the chair of Japanese National Body for ISO/TC68 (Financial Services), and a core member of the Cryptography Research and Evaluation Committees (CRYPTREC). He was a director of the International Association for Cryptologic Research (IACR) and the chair of the IEICE Technical Committee on Information Security and served as an associate member of the Science Council of Japan (SCJ). He received the IEICE Achievement Award, the DoCoMo Mobile Science Award, the Culture of Information Security Award, the MEXT Prize for Science and Technology, and the Fuji Sankei Business Eye Award.



Christian Rossow graduated in Computer Science in 2013 at the VU Amsterdam, The Netherlands. Since 2014, he leads the "System Security" Research Group at Saarland University, Germany. He also holds a Guest Associate Professorship at Yokohama National University, Japan. His research focuses

are binary analysis, malicious software and network security.