MAR-10135536-17 – North Korean Trojan: KEYMARBLE

us-cert.gov/ncas/analysis-reports/AR18-221A

Notification

This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of ar any information contained within. The DHS does not endorse any commercial product or service, referenced in this bulletin or otherwise.

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeabl in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distrib restriction. For more information on the Traffic Light Protocol, see http://www.us-cert.gov/tlp.

Summary

Description

This Malware Analysis Report (MAR) is the result of analytic efforts between Department of Homeland Security (DHS) and the Federal Bureau of (FBI). Working with U.S. Government partners, DHS and FBI identified Trojan malware variants used by the North Korean government. This malw been identified as KEYMARBLE. The U.S. Government refers to malicious cyber activity by the North Korean government as HIDDEN COBRA. F information on HIDDEN COBRA activity, visit https://www.us-cert.gov/hiddencobra.

DHS and FBI are distributing this MAR to enable network defense and reduce exposure to North Korean government malicious cyber activity.

This MAR includes malware descriptions related to HIDDEN COBRA, suggested response actions and recommended mitigation techniques. Use administrators should flag activity associated with the malware, report the activity to the DHS National Cybersecurity and Communications Integra (NCCIC) or the FBI Cyber Watch (CyWatch), and give the activity the highest priority for enhanced mitigation.
This malware report contains analysis of one 32-bit Windows executable file, identified as a Remote Access Trojan (RAT). This malware is capab device configuration data, downloading additional files, executing commands, modifying the registry, capturing screen shots, and exfiltrating data.

For a downloadable copy of IOCs, see:

MAR-10135536-17.stix

Submitted Files (1)

e23900b00ffd67cd8dfa3283d9ced691566df6d63d1d46c95b22569b49011f09 (704d491c155aad996f16377a35732c...)

IPs (3)

100.43.153.60

104.194.160.59

212.143.21.43

Findings

e23900b00ffd67cd8dfa3283d9ced691566df6d63d1d46c95b22569b49011f09

Tags

trojan

Details

Name	704d491c155aad996f16377a35732cb4
Size	126976 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	704d491c155aad996f16377a35732cb4
SHA1	d1410d073a6df8979712dd1b6122983f66d5bef8
SHA256	e23900b00ffd67cd8dfa3283d9ced691566df6d63d1d46c95b22569b49011f09
SHA512	0092900bf4ca71c17a3caa225a4d7dcc60c7b58f7ffd173f46731db7f696e34b2e752aefaf9cedc27fe76fe317962a394f1be2e59bd0cffaa
ssdeep	3072:IDdXEYhXxS550wwiY0Pe6Q1vLo4lJnCtea:EXEEXxcQxZ
Entropy	6.264656

Antivirus

Ahnlab	Trojan/Win32.Agent
Antiy	Trojan/Win32.AGeneric

Avira	TR/Agent.rhagj
BitDefender	Trojan.GenericKD.4837544
ESET	a variant of Win32/NukeSped.H trojan
Emsisoft	Trojan.GenericKD.4837544 (B)
Ikarus	Trojan.Agent
K7	Trojan (0050e4401)
McAfee	GenericRXBP-FF!704D491C155A
NANOAV	Trojan.Win32.Agent.eqcfki
NetGate	Trojan.Win32.Malware
Quick Heal	Trojan.IGENERIC
Symantec	Process timed out
TACHYON	Trojan/W32.Agent.126976.CTO
Zillya!	Trojan.NukeSped.Win32.5

Yara Rules

hidden_cobra_consolidated.yara	rule rsa_modulus { meta: Author="NCCIC trusted 3rd party" Incident="10135536" Date = "2018/04/19" cate "hidden_cobra" family = "n/a" description = "n/a" strings: $n = "bc9b75a31177587245305cd418b8df78652d1c03e9da0cfc910d6d38ee4191d40" condition: (uint16(0) == (uint16(uint32(0x3c)) == 0x4550) and any of them }

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2017-04-12 11:16:04-04:00
Import Hash	fc7dab4d20f23681313b91eba653aa21

PE Sections

MD5	Name	Raw Size	Entropy
47f6fac41465e01dda5eac297ab250db	header	4096	0.627182
30d34a8f4c29d7c2feb0f6e2b102b0a4	.text	94208	6.633409
77f4a11d375f0f35b64a0c43fab947b8	.rdata	8192	5.054283
d4364f6d2f55a37f0036e9e0dc2c6a2b	.data	20480	4.416980

Packers/Compilers/Cryptors

Microsoft Visual C++ v6.0

Relationships

e23900b00f...	Connected_To	104.194.160.59
e23900b00f...	Connected_To	212.143.21.43
e23900b00f...	Connected_To	100.43.153.60

Description

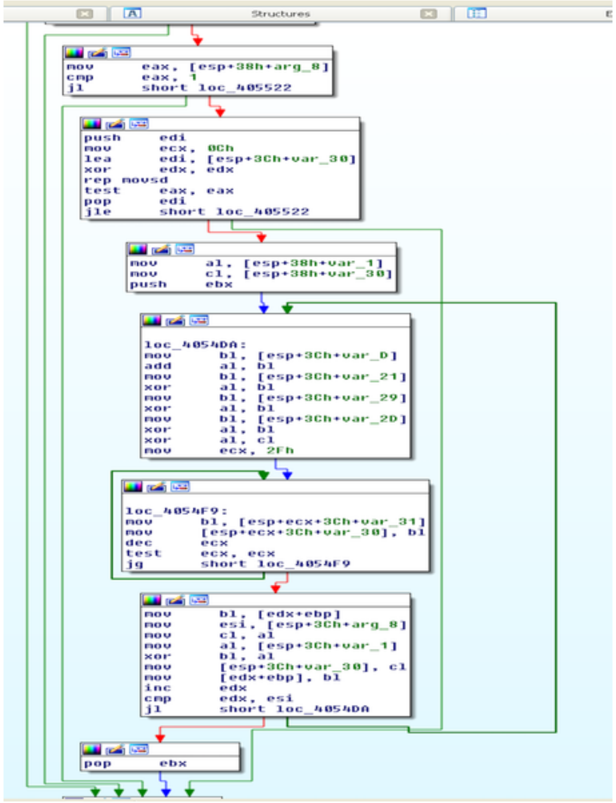
This application is a malicious 32-bit Windows executable file, which functions as a RAT. When executed, it de-obfuscates its application program (APIs) and using port 443, attempts to connect to the hard-coded IP addresses listed below. After connecting, the malware waits for further instru

--Begin hard-coded IP addresses--
100.43.153.60
104.194.160.59
212.143.21.43
--End hard-coded IP addresses--

Static analysis reveals that this RAT uses a customized XOR cryptographic algorithm displayed in Figure 1 to secure its data transfers and comm (C2) sessions. It is designed to accept instructions from the remote server to perform the following functions:

--Begin functions--
Download and upload files
Execute secondary payloads
Execute shell commands
Terminate running processes
Delete files
Search files
Set file attributes
Create registry entries for storing data:(HKEY_CURRENT_USER\SOFTWARE\Microsoft\WABE\DataPath)
Collect device information from installed storage devices (disk free space and their type)
List running processes information
Capture screenshots
Collect and send information about the victim's system (operating system, CPU, MAC address, computer name, language settings, list of disk dev type, time elapsed since the system was started, and unique identifier of the victim's system)
--End functions--

Screenshots



```
mov     eax, [esp+38h+arg_8]
cmp     eax, 1
jl      short loc_405522
```

```
push    edi
mov     ecx, 0Ch
lea     edi, [esp+3Ch+var_30]
xor     edx, edx
rep movsd
test    eax, eax
pop     edi
jle     short loc_405522
```

```
mov     al, [esp+38h+var_1]
mov     cl, [esp+38h+var_30]
push    ebx
```

```
loc_4054DA:
mov     bl, [esp+3Ch+var_D]
add     al, bl
mov     bl, [esp+3Ch+var_21]
xor     al, bl
mov     bl, [esp+3Ch+var_29]
xor     al, bl
mov     bl, [esp+3Ch+var_2D]
xor     al, bl
xor     al, cl
mov     ecx, 2Fh
```

```
loc_4054F9:
mov     bl, [esp+ecx+3Ch+var_31]
mov     [esp+ecx+3Ch+var_30], bl
dec     ecx
test    ecx, ecx
jg      short loc_4054F9
```

```
mov     bl, [edx+ebp]
mov     esi, [esp+3Ch+arg_8]
mov     cl, al
mov     al, [esp+3Ch+var_1]
xor     bl, al
mov     [esp+3Ch+var_30], cl
mov     [edx+ebp], bl
inc     edx
cmp     edx, esi
jl      short loc_4054DA
```

```
pop     ebx
```

Figure 1 - Screenshot of the cryptographic algorithms the malware used to secure its data transfers and C2 sessions.

100.43.153.60

Ports

443 TCP

Whois

Domain Name: KRYPT.COM
Registry Domain ID: 4620809_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2016-02-25T03:39:29Z
Creation Date: 1998-05-04T04:00:00Z
Registry Expiry Date: 2024-05-03T04:00:00Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: 480-624-2505
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: NS1.CF.KRYPT.COM
Name Server: NS2.CF.KRYPT.COM
Name Server: NS3.CF.KRYPT.COM

```
DNSSEC: signedDelegation
DNSSEC DS Data: 2371 13 2 503AEB51F773BBCA00DB982C938895EF147DDC7D48A4E1E6FD0FE5BE7B98DA0D
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
Last update of whois database: 2018-06-28T02:39:11Z
```

Relationships

```
 100.43.153.60    Connected_From    e23900b00ffd67cd8dfa3283d9ced691566df6d63d1d46c95b22569b49011f09
```

104.194.160.59

Ports

```
    443 TCP
```

Whois

```
Domain Name: SERVPAC.COM
Registry Domain ID: 81803816_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2013-12-27T04:46:10Z
Creation Date: 2001-12-31T08:29:34Z
Registry Expiry Date: 2018-12-31T08:29:34Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: 480-624-2505
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: NS1.SERVPAC.COM
Name Server: NS2.SERVPAC.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
Last update of whois database: 2018-06-28T02:40:41Z
```

Relationships

```
 104.194.160.59    Connected_From    e23900b00ffd67cd8dfa3283d9ced691566df6d63d1d46c95b22569b49011f09
```

212.143.21.43

Ports

```
    443 TCP
```

Whois

```
netnum:        212.143.21.0 - 212.143.21.63
netname:        Nana10-LAN
descr:         Nana10-LAN
country:        IL
admin-c:        NV6695-RIPE
tech-c:         NV6695-RIPE
status:         ASSIGNED PA
mnt-by:         NV-MNT-RIPE
created:        2011-02-17T09:16:56Z
last-modified: 2011-02-17T09:16:57Z
source:         RIPE

person:         Nana 10 LTD
address:        1 Korazin str
address:        Givataim, Israel, 53583
mnt-by:         NV-MNT-RIPE
phone:          +972-73-7992000
fax-no:         +972-73-7992220
e-mail:         domains@nana10.net.il
nic-hdl:        NV6695-RIPE
created:        2010-08-04T09:51:11Z
last-modified: 2011-02-17T09:01:21Z
source:         RIPE

% Information related to '212.143.0.0/16AS1680'

route:         212.143.0.0/16
descr:         013 Netvision Network
origin:        AS1680
mnt-by:         NV-MNT-RIPE
created:        1970-01-01T00:00:00Z
```

last-modified: 2009-03-26T10:55:12Z
source: RIPE
Relationships

212.143.21.43	Connected_From	e23900b00ffd67cd8dfa3283d9ced691566df6d63d1d46c95b22569b49011f09

Relationship Summary

e23900b00f...	Connected_To	104.194.160.59
e23900b00f...	Connected_To	212.143.21.43
e23900b00f...	Connected_To	100.43.153.60
100.43.153.60	Connected_From	e23900b00ffd67cd8dfa3283d9ced691566df6d63d1d46c95b22569b49011f09
104.194.160.59	Connected_From	e23900b00ffd67cd8dfa3283d9ced691566df6d63d1d46c95b22569b49011f09
212.143.21.43	Connected_From	e23900b00ffd67cd8dfa3283d9ced691566df6d63d1d46c95b22569b49011f09

Recommendations

NCCIC would like to remind users and administrators to consider using the following best practices to strengthen the security posture of their orga systems. Any configuration changes should be reviewed by system owners and administrators prior to implementation to avoid unwanted impacts

- Maintain up-to-date antivirus signatures and engines.
- Keep operating system patches up-to-date.
- Disable File and Printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Restrict users' ability (permissions) to install and run unwanted software applications. Do not add users to the local administrators group unl
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.
- Enable a personal firewall on agency workstations, configured to deny unsolicited connection requests.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumbdrives, external drives, CDs, etc.).
- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats and implement appropriate ACLs.

Additional information on malware incident prevention and handling can be found in NIST's Special Publication 800-83, **Guide to Malware Incide Handling for Desktops and Laptops.**

Contact Information

NCCIC continuously strives to improve its products and services. You can help by answering a very short series of questions about this product a URL: https://us-cert.gov/forms/feedback/

Document FAQ

What is a MAR? A Malware Analysis Report (MAR) is intended to provide organizations with more detailed malware analysis acquired via manua engineering. To request additional analysis, please contact US-CERT and provide information regarding the level of desired analysis.

Can I submit malware to NCCIC? Malware samples can be submitted via three methods:

- Web: https://malware.us-cert.gov
- E-Mail: submit@malware.us-cert.gov
- FTP: ftp.malware.us-cert.gov (anonymous)

NCCIC encourages you to report any suspicious activity, including cybersecurity incidents, possible malicious code, software vulnerabilities, and p scams. Reporting forms can be found on US-CERT's homepage at www.us-cert.gov.

Revisions

August 9, 2018: Initial version

Please share your thoughts.

We recently updated our anonymous product survey; we'd welcome your feedback.