Alert (TA17-164A)

TLP:WHITE

HIDDEN COBRA – North Korea's DDoS Botnet Infrastructure

Original release date: June 13, 2017

Systems Affected

Networked Systems

Overview

This joint Technical Alert (TA) is the result of analytic efforts between the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). This alert provides technical details on the tools and infrastructure used by cyber actors of the North Korean government to target the media, aerospace, financial, and critical infrastructure sectors in the United States and globally. Working with U.S. Government partners, DHS and FBI identified Internet Protocol (IP) addresses associated with a malware variant, known as DeltaCharlie, used to manage North Korea's distributed denial-of-service (DDoS) botnet infrastructure. This alert contains indicators of compromise (IOCs), malware descriptions, network signatures, and host-based rules to help network defenders detect activity conducted by the North Korean government. The U.S. Government refers to the malicious cyber activity by the North Korean government as HIDDEN COBRA.

If users or administrators detect the custom tools indicative of HIDDEN COBRA, these tools should be immediately flagged, reported to the DHS National Cybersecurity Communications and Integration Center (NCCIC) or the FBI Cyber Watch (CyWatch), and given highest priority for enhanced mitigation. This alert identifies IP addresses linked to systems infected with DeltaCharlie malware and provides descriptions of the malware and associated malware signatures. DHS and FBI are distributing these IP addresses to enable network defense activities and reduce exposure to the DDoS command-and-control network. FBI has high confidence that HIDDEN COBRA actors are using the IP addresses for further network exploitation.

This alert includes technical indicators related to specific North Korean government cyber operations and provides suggested response actions to those indicators, recommended mitigation techniques, and information on reporting incidents to the U.S. Government.

For a downloadable copy of IOCs, see:

- IOCs (.csv)
- IOCs (STIX)

Description

Since 2009, HIDDEN COBRA actors have leveraged their capabilities to target and compromise a range of victims; some intrusions have resulted in the exfiltration of data while others have been disruptive in nature. Commercial reporting has referred to this activity as Lazarus Group[1] and Guardians of Peace.[2] DHS and FBI assess that HIDDEN COBRA actors will continue to use cyber operations to advance their government's military and strategic objectives. Cyber analysts are encouraged to review the information provided in this alert to detect signs of malicious network activity.

Tools and capabilities used by HIDDEN COBRA actors include DDoS botnets, keyloggers, remote access tools (RATs), and wiper malware. Variants of malware and tools used by HIDDEN COBRA actors include Destover,[3] Wild Positron/Duuzer,[4] and Hangman.[5] DHS has previously released Alert TA14-353A,[6] which contains additional details on the use of a

TLP:WHITE

server message block (SMB) worm tool employed by these actors. Further research is needed to understand the full breadth of this group's cyber capabilities. In particular, DHS recommends that more research should be conducted on the North Korean cyber activity that has been reported by cybersecurity and threat research firms.

HIDDEN COBRA actors commonly target systems running older, unsupported versions of Microsoft operating systems. The multiple vulnerabilities in these older systems provide cyber actors many targets for exploitation. These actors have also used Adobe Flash player vulnerabilities to gain initial entry into users' environments.

HIDDEN COBRA is known to use vulnerabilities affecting various applications. These vulnerabilities include:

- CVE-2015-6585: Hangul Word Processor Vulnerability
- CVE-2015-8651: Adobe Flash Player 18.0.0.324 and 19.x Vulnerability
- CVE-2016-0034: Microsoft Silverlight 5.1.41212.0 Vulnerability
- CVE-2016-1019: Adobe Flash Player 21.0.0.197 Vulnerability
- CVE-2016-4117: Adobe Flash Player 21.0.0.226 Vulnerability

We recommend that organizations upgrade these applications to the latest version and patch level. If Adobe Flash or Microsoft Silverlight is no longer required, we recommend that those applications be removed from systems.

The indicators provided with this alert include IP addresses determined to be part of the HIDDEN COBRA botnet infrastructure, identified as DeltaCharlie. The DeltaCharlie DDoS bot was originally reported by Novetta in their 2016 Operation Blockbuster Malware Report.[7] This malware has used the IP addresses identified in the accompanying .csv and .stix files as both source and destination IPs. In some instances, the malware may have been present on victims' networks for a significant period.

Technical Details

DeltaCharlie is a DDoS tool used by HIDDEN COBRA actors, and is referenced and detailed in Novetta's Operation Blockbuster Destructive Malware report. The information related to DeltaCharlie from the Operation Blockbuster Destructive Malware report should be viewed in conjunction with the IP addresses listed in the .csv and .stix files provided within this alert. DeltaCharlie is a DDoS tool capable of launching Domain Name System (DNS) attacks, Network Time Protocol (NTP) attacks, and Character Generation Protocol attacks. The malware operates on victims' systems as a svchost-based service and is capable of downloading executables, changing its own configuration, updating its own binaries, terminating its own processes, and activating and terminating denial-of-service attacks. Further details on the malware can be found in Novetta's report.

Detection and Response

HIDDEN COBRA IOCs related to DeltaCharlie are provided within the accompanying .csv and .stix files of this alert. DHS and FBI recommend that network administrators review the IP addresses, file hashes, network signatures, and YARA rules provided, and add the IPs to their watchlist to determine whether malicious activity has been observed within their organization.

When reviewing network perimeter logs for the IP addresses, organizations may find numerous instances of these IP addresses attempting to connect to their systems. Upon reviewing the traffic from these IP addresses, system owners may find that some traffic corresponds to malicious activity and some to legitimate activity. System owners are also advised to run the YARA tool on any system they suspect to have been targeted by HIDDEN

COBRA actors. Additionally, the appendices of this report provide network signatures to aid in the detection and mitigation of HIDDEN COBRA activity.

Network Signatures and Host-Based Rules

This section contains network signatures and host-based rules that can be used to detect malicious activity associated with HIDDEN COBRA actors. Although created using a comprehensive vetting process, the possibility of false positives always remains. These signatures and rules should be used to supplement analysis and should not be used as a sole source of attributing this activity to HIDDEN COBRA actors.

Network Signatures

alert tcp any any -> any any (msg:"DPRK_HIDDEN_COBRA_DDoS_HANDSHAKE_SUCCESS"; dsize:6; flow:established,to_server; content:"|18 17 e9 e9 e9 e9|"; fast_pattern:only; sid:1; rev:1;)

---

alert tcp any any -> any any (msg:"DPRK_HIDDEN_COBRA_Botnet_C2_Host_Beacon"; flow:established,to_server; content:"|1b 17 e9 e9 e9 e9|"; depth:6; fast_pattern; sid:1; rev:1;)

YARA Rules

"strings:

$rsaKey = {7B 4E 1E A7 E9 3F 36 4C DE F4 F0 99 C4 D9 B7 94

A1 FF F2 97 D3 91 13 9D C0 12 02 E4 4C BB 6C 77

48 EE 6F 4B 9B 53 60 98 45 A5 28 65 8A 0B F8 39

73 D7 1A 44 13 B3 6A BB 61 44 AF 31 47 E7 87 C2

AE 7A A7 2C 3A D9 5C 2E 42 1A A6 78 FE 2C AD ED

39 3F FA D0 AD 3D D9 C5 3D 28 EF 3D 67 B1 E0 68

3F 58 A0 19 27 CC 27 C9 E8 D8 1E 7E EE 91 DD 13

B3 47 EF 57 1A CA FF 9A 60 E0 64 08 AA E2 92 D0}

condition: any of them"

"strings:

$STR1 = "Wating" wide ascii

$STR2 = "Reamin" wide ascii

$STR3 = "laptos" wide ascii

condition: (uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) == 0x46445025 or uint32(1) == 0x6674725C) and 2 of them}"

"strings:

$randomUrlBuilder = { 83 EC 48 53 55 56 57 8B 3D ?? ?? ?? ?? 33 C0 C7 44 24 28 B4 6F 41 00 C7 44 24 2C B0 6F 41 00 C7 44 24 30 AC 6F 41 00 C7 44 24 34 A8 6F 41 00 C7 44 24 38 A4 6F 41 00 C7 44 24 3C A0 6F 41 00 C7 44 24 40 9C 6F 41 00 C7 44 24 44 94 6F 41 00 C7 44 24 48 8C 6F 41 00 C7 44 24 4C 88 6F 41 00 C7 44 24 50 80 6F 41 00 89 44 24 54 C7 44 24 10 7C 6F 41 00 C7 44 24 14 78 6F 41 00 C7 44 24 18 74 6F 41 00 C7 44 24 1C 70 6F 41 00 C7 44 24 20 6C 6F 41 00 89 44 24 24 FF D7 99 B9 0B 00 00 00 F7 F9 8B 74 94 28 BA 9C 6F 41 00 66 8B 06 66 3B 02 74 34 8B FE 83 C9 FF 33 C0 8B 54 24 60 F2 AE 8B 6C 24 5C A1 ?? ?? ?? ?? F7 D1 49 89 45 00 8B FE 33 C0 8D 5C 11 05 83 C9 FF 03 DD F2 AE F7 D1 49 8B FE 8B D1 EB 78 FF D7 99 B9 05 00 00 00 8B 6C 24 5C F7 F9 83 C9 FF 33 C0 8B 74 94 10 8B 54 24 60 8B FE F2 AE F7 D1 49 BF 60 6F 41 00 8B D9 83 C9 FF F2 AE F7 D1 8B C2 49 03 C3 8B FE 8D 5C 01 05 8B 0D ?? ?? ?? ?? 89 4D 00 83 C9 FF 33 C0 03 DD F2 AE F7 D1 49 8D 7C 2A 05 8B D1 C1 E9 02 F3 A5 8B CA 83 E1 03 F3 A4 BF 60 6F 41 00 83 C9 FF F2 AE F7 D1 49 BE 60 6F 41 00 8B D1 8B FE 83 C9 FF 33 C0 F2 AE F7 D1 49 8B FB 2B F9 8B CA 8B C1 C1 E9 02 F3 A5 8B C8 83 E1 03 F3 A4 8B 7C 24 60 8D 75 04 57 56 E8 ?? ?? ?? ?? 83 C4 08 C6 04 3E 2E 8B C5 C6 03 00 5F 5E 5D 5B 83 C4 48 C3 }

condition: $randomUrlBuilder"

Impact

A successful network intrusion can have severe impacts, particularly if the compromise becomes public and sensitive information is exposed. Possible impacts include:

- temporary or permanent loss of sensitive or proprietary information,
- disruption to regular operations,
- financial losses incurred to restore systems and files, and
- potential harm to an organization's reputation.

Solution

Mitigation Strategies

Network administrators are encouraged to apply the following recommendations, which can prevent as many as 85 percent of targeted cyber intrusions. The mitigation strategies provided may seem like common sense. However, many organizations fail to use these basic security measures, leaving their systems open to compromise:

1. **Patch applications and operating systems** – Most attackers target vulnerable applications and operating systems. Ensuring that applications and operating systems are patched with the latest updates greatly reduces the number of exploitable entry points available to an attacker. Use best practices when updating software and patches by only downloading updates from authenticated vendor sites.
2. **Use application whitelisting** – Whitelisting is one of the best security strategies because it allows only specified programs to run while blocking all others, including malicious software.
3. **Restrict administrative privileges** – Threat actors are increasingly focused on gaining control of legitimate credentials, especially credentials associated with highly privileged accounts. Reduce privileges to only those needed for a user's duties. Separate administrators into privilege tiers with limited access to other tiers.
4. **Segment networks and segregate them into security zones** – Segment networks into logical enclaves and restrict host-to-host communications paths. This helps protect sensitive information and critical services, and limits damage from network perimeter breaches.

5. **Validate input** – Input validation is a method of sanitizing untrusted input provided by users of a web application. Implementing input validation can protect against the security flaws of web applications by significantly reducing the probability of successful exploitation. Types of attacks possibly averted include Structured Query Language (SQL) injection, cross-site scripting, and command injection.
6. **Use stringent file reputation settings** – Tune the file reputation systems of your anti-virus software to the most aggressive setting possible. Some anti-virus products can limit execution to only the highest reputation files, stopping a wide range of untrustworthy code from gaining control.
7. **Understand firewalls** – Firewalls provide security to make your network less susceptible to attack. They can be configured to block data and applications from certain locations (IP whitelisting), while allowing relevant and necessary data through.

Response to Unauthorized Network Access

Enforce your security incident response and business continuity plan. It may take time for your organization's IT professionals to isolate and remove threats to your systems and restore normal operations. Meanwhile, you should take steps to maintain your organization's essential functions according to your business continuity plan. Organizations should maintain and regularly test backup plans, disaster recovery plans, and business continuity procedures.

Contact DHS or your local FBI office immediately. To report an intrusion and request resources for incident response or technical assistant, you are encouraged to contact DHS NCCIC (NCCICCustomerService@hq.dhs.gov or 888-282-0870), the FBI through a local field office, or the FBI's Cyber Division (CyWatch@fbi.gov or 855-292-3937).

Protect Against SQL Injection and Other Attacks on Web Services

To protect against code injections and other attacks, system operators should routinely evaluate known and published vulnerabilities, periodically perform software updates and technology refreshes, and audit external-facing systems for known web application vulnerabilities. They should also take the following steps to harden both web applications and the servers hosting them to reduce the risk of network intrusion via this vector.

- Use and configure available firewalls to block attacks.
- Take steps to secure Windows systems, such as installing and configuring Microsoft's Enhanced Mitigation Experience Toolkit (EMET) and Microsoft AppLocker.
- Monitor and remove any unauthorized code present in any www directories.
- Disable, discontinue, or disallow the use of Internet Control Message Protocol (ICMP) and Simple Network Management Protocol (SNMP) as much as possible.
- Remove unnecessary HTTP verbs from web servers. Typical web servers and applications only require GET, POST, and HEAD.
- Where possible, minimize server fingerprinting by configuring web servers to avoid responding with banners identifying the server software and version number.
- Secure both the operating system and the application.
- Update and patch production servers regularly.
- Disable potentially harmful SQL-stored procedure calls.
- Sanitize and validate input to ensure that it is properly typed and does not contain escaped code.
- Consider using type-safe stored procedures and prepared statements.
- Audit transaction logs regularly for suspicious activity.
- Perform penetration testing on web services.

- Ensure error messages are generic and do not expose too much information.

Permissions, Privileges, and Access Controls

System operators should take the following steps to limit permissions, privileges, and access controls.

- Reduce privileges to only those needed for a user's duties.
- Restrict users' ability (permissions) to install and run unwanted software applications, and apply the principle of "Least Privilege" to all systems and services. Restricting these privileges may prevent malware from running or limit its capability to spread through the network.
- Carefully consider the risks before granting administrative rights to users on their own machines.
- Scrub and verify all administrator accounts regularly.
- Configure Group Policy to restrict all users to only one login session, where possible.
- Enforce secure network authentication, where possible.
- Instruct administrators to use non-privileged accounts for standard functions such as web browsing or checking webmail.
- Segment networks into logical enclaves and restrict host-to-host communication paths. Containment provided by enclaving also makes incident cleanup significantly less costly.
- Configure firewalls to disallow Remote Desktop Protocol (RDP) traffic coming from outside of the network boundary, except for in specific configurations such as when tunneled through a secondary virtual private network (VPN) with lower privileges.
- Audit existing firewall rules and close all ports that are not explicitly needed for business. Specifically, carefully consider which ports should be connecting outbound versus inbound.
- Enforce a strict lockout policy for network users and closely monitor logs for failed login activity. Failed login activity can be indicative of failed intrusion activity.
- If remote access between zones is an unavoidable business need, log and monitor these connections closely.
- In environments with a high risk of interception or intrusion, organizations should consider supplementing password authentication with other forms of authentication such as challenge/response or multifactor authentication using biometric or physical tokens.

Logging Practices

System operators should follow these secure logging practices.

- Ensure event logging, including applications, events, login activities, and security attributes, is turned on or monitored for identification of security issues.
- Configure network logs to provide adequate information to assist in quickly developing an accurate determination of a security incident.
- Upgrade PowerShell to new versions with enhanced logging features and monitor the logs to detect usage of PowerShell commands, which are often malware-related.
- Secure logs in a centralized location and protect them from modification.
- Prepare an incident response plan that can be rapidly administered in case of a cyber intrusion.

References

- [1] IBM. Actor Lazarus Group – Blog Post by IBM X-Force Exchange.

TLP:WHITE

- [2] Alien Vault. Operation Blockbuster Unveils the Actors Behind the Sony Attacks.
- [3] Symantec. Destover: Destructive Malware has links back to attacks on South Korea.
- [4] Symantec. Duuzer back door Trojan targets South Korea to take over computers.
- [5] FireEye. Zero-Day HWP Exploit.
- [6] US-CERT. Alert (TA14-353A) Targeted Destructive Malware. Original Release Date: 12/19/2014 | Last revised: 9/30/2016
- [7] Novetta. Operation Blockbuster Destructive Malware Report.

Revisions

- June 13, 2017: Initial Release

TLP:WHITE

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu