NTT Security

GTIC Monthly Threat Report

June 2018

Contents

North Korean Hacker Group HIDDEN COBRA Still in Business

Lead Analyst: Danika Blessman

Hidden Cobra, also known as The Lazarus Group, active since at least 2009, is clearly continuing campaigns against global targets. The U.S. Federal Bureau of Investigation (FBI) and the U.S. Department of Homeland Security (DHS) have released a dozen or so reports over the past year concerning the group's activities.

Unlike portions of Covellite's operations targeting U.S. infrastructure, discussed in a later article, Hidden Cobra continues operations against U.S. and global targets. Of note, many researchers believe that Covellite is also thought to have ties to the government of North Korea because of overlapping infrastructure with Hidden Cobra, though this has yet to be definitively proven.

The most recent report, a joint analytic effort between the FBI and DHS, details a new malware variant called TypeFrame, suspected of being leveraged in Hidden Cobra operations. The malware analysis report covered 11 samples related to the threat, including executable files and malicious Word documents containing VBA macros. The report goes on to state that the malware has the capability to download and install additional malware and Remote Access Trojans (RATs) and call back to command and control (C2) servers for additional instructions. TypeFrame can also modify characteristics of victim firewalls, allowing incoming connections from the malware C2 server.

In addition to campaigns observed in the U.S., Hidden Cobra continues operations against global targets, including South Korean cryptocurrency exchange, Bithumb, possibly in efforts to gain funds for other efforts.

In addition, larger campaigns like Operation GhostSecret, discovered to have been conducting reconnaissance on organizations in multiple industries across at least 17 countries, suggest there is still unknown infrastructure, and likely additional operations yet to be discovered.

The North Korean cyber threat continues to evolve, as threat actors improve their skills and stealth. Combined with intent and motivation, especially if they feel threatened in their position in a given scenario, this advancement in their skillset requires all of us to remain vigilant.

References

U.S. CERT: HIDDEN COBRA - North Korean Malicious Cyber Activity

Trickbot Campaign Leveraging Double Kill Vulnerability

Lead Analyst: Terrance DeJesus

On 18 April 2018, Qihoo 360's Core Security division detected what they believed to be a zero-day vulnerability called Double Kill (CVE-2018-8174) being exploited in the wild. Researchers recorded, analyzed and submitted the activity to Microsoft, who confirmed the activity on 20 April 2018.

Double Kill is a remote code execution vulnerability that exists in the VBScript engine and how the engine handles certain objects in memory. In short, a use-after-free (UAF) vulnerability can be exploited with specific code due to incorrect object lifetime handling in the *Class_Terminate* VBScript method, causing freed objects to be referenced after the exploit, ultimately allowing payload execution.

Practical Attack Cycle

Until the discovery of Double Kill, Visual Basic vulnerabilities could only be leveraged inside Internet Explorer (IE), Internet Information Servers (IIS) or Windows Script Host (WSH), limiting the scope of this attack. As of 26 June 2018, Internet Explorer only accounted for 12.75 percent of all web browser usage but is installed by default on all Windows operating systems up to Windows 7 and Windows Server 2008 R2. As a result, attackers see exploiting this vulnerability as a prime opportunity.

Malspam, one of the most common and effective infection chains, involves sending emails with malicious attachments to potential victims. In this case, the malicious attachment sends requests to a remote server to download an HTML page containing malicious VBScript code. This code spawns *mshta.exe* as a process to handle this object.

Leveraging *mshta* is not uncommon in cyber attacks, as it is an effective method for executing JavaScript or VBScript, possessing the capability to bypass application whitelisting solutions and browser security settings, because *mshta* executes outside of IE's security context.

Once *mshta.exe* is spawned it is chosen as the OLE server to run the script requested, unrestricted, allowing attackers to call Windows *ShellExecute* API to launch a malicious payload. Regardless of whether IE is the default browser, if the victim machine is running Windows 7 or Windows Server 2008 R2 and below, the machine is potentially vulnerable to CVE-2018-8174.

Leave it to Trickbot Actors to Start the Trend

Since the release of this vulnerability and it subsequent integration into ThreadKit, a popular document exploit builder, GTIC researchers expected usage in malspam campaigns was inevitable as vulnerabilities used in common malspam such as Trickbot, Emotet, and LokiBot have depended on the use of ThreadKit to continually recycle effective vulnerabilities such as CVE-2017-11882 in their campaigns. Prior to 26 June 2018, threat actors' use of CVE-2018-8174 were limited to RIG, Magnitude and GrandSoft exploit kit activity.

On 16 June 2018, another researcher reported emails containing the subject "Barclays Secured Message: New Message Received". The email contained a link to a URL which downloaded a VBS file to the victim's machine. The downloaded file exploits CVE-2018-8174, and then runs a PowerShell command to download Trickbot from aasoftbd[.]org or cyprus[.]com and launch itself.

GTIC researchers continuously analyze Trickbot malspam campaigns, and with the integration of CVE-2018-8174, GTIC researchers fully expect to see other malspam campaigns leveraging ThreadKit in an attempt to exploit this vulnerability.

NTT Security recommends the latest Microsoft patch to mitigate your risk from this vulnerability.

References:
Mitre: Mshta technique
Article: Double Kill VBScript zero-day exploit
Article: CVE-2018-8174
Article: Fake Barclays Message
Article: RIG exploit kit using CVE-2018-8174 to deliver Monero miner

Cisco Adaptive Security Appliance (ASA) Vulnerability

Lead Analyst: Jose Hernandez

Threat Status: High

CVE-2018-0296

Severity: **High** (CVSS: 8.6)

Date: 6 June 2018

Remediation Details: Cisco has released free software updates which address this vulnerability

Affected Versions:

- 3000 Series Industrial Security Appliance (ISA)
- ASA 1000V Cloud Firewall
- ASA 5500 Series Adaptive Security Appliances
- ASA 5500-X Series Next-Generation Firewalls
- ASA Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers
- Adaptive Security Virtual Appliance (ASAv)
- Firepower 2100 Series Security Appliance
- Firepower 4100 Series Security Appliance
- Firepower 9300 ASA Security Module
- FTD Virtual (FTDv)

Analyst Note: Researchers discovered a vulnerability in the web interface of the Cisco Adaptive Security Appliance (ASA) which could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. The vulnerability also allows attackers to view sensitive system information without authentication through Directory traversals. Attackers are currently exploiting this vulnerability to enumerate usernames on the system. The vulnerability exists because of a lack of proper input validation of the HTTP URL. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device.

North Korean Cyber Activities Continue

Lead Analyst: Danika Blessman

Historically, suspected state-sponsored North Korean threat actors have conducted cyber operations coinciding with major state events such as missile tests or meaningful national dates.

Also, from an historical perspective, North Korean cyber operations are typically driven by several primary motives: financial gain, information gathering, and retribution for perceived injustices.

The question is – did the time leading up to the G7 summit, and the Singapore summit between the U.S. and North Korea (8-9 June and 12 June respectively) coincide with North Korean cyber operations?

On the surface at least, even a quick review of open source intelligence sources suggests an increase in cyber operations from suspected North Korean threat actors over the last few months, including hacks leveraging an ActiveX zero-day, and several spear-phishing operations using the U.S./N.K. summit as the subject, tempting end-users to click through.

Security researchers and law enforcement officials continue to speculate as to what exactly is going on *under* the surface. Obvious attacks, such as those against energy sector targets in operations under Covellite – a suspected North Korean threat group targeting organizations in the energy and critical infrastructure sectors – may obscure or overshadow other attacks. Interestingly, Covellite appears to have ceased all activity against U.S. targets while continuing operations against targets in other nations, including those in Europe and East Asia.

Most other North Korean cyber operations continue and will likely not subside.

In fact, operations were identified as recently as 14 June, as the US-CERT released additional indicators of compromise of suspected Hidden Cobra Trojan activity, called TYPEFRAME, discussed a bit further in the first article of this report.

Although any industry could be a target, organizations in the energy sector should be particularly aware of the threat, most recently emanating from Covellite. Additionally, in late May, the FBI and DHS jointly issued two separate technical advisories detailing the Joanap and Brambul malware families, in use since at least 2009, targeting multiple sectors worldwide including media, finance and critical infrastructure.

It is crucial that organizations remain vigilant and engage in best security practices to reduce risk throughout their environments.

References:

Article: North Korean hacking group Covellite abandons US targets
Article: Joanap and Brambul malware families
Article: G7 members call for North Korean nuclear disarmament

About GTIC

The NTT Security GTIC protects and informs NTT Group clients through security threat research, vulnerability analysis and the development of effective countermeasures. For more information, including vulnerability disclosures, threat reports and white papers, visit the resource page on www.nttsecurity.com or our blog.