GTIC Monthly Threat Report

July 2017

Name	**[GTIC Monthly Threat Report] July 2017**
Owner	**NTT Security [GTIC/TICT]**
Status	APPROVED
Classification	UNCLASSIFIED-EXTERNAL
Version	V 1.0
Date	**20 July 2017**
Review	31 July 2017

Contents

1 Observations: Cyber Kill Chain

The NTT Security Global Threat Intelligence Center (GTIC) analyzed MSSP observations starting with a high-level overview of detections correlated to Lockheed Martin's Cyber Kill Chain. In doing so, analysts determined 95 percent of detections correlated to reconnaissance. Once this determination was made, analysts shifted their focus to the remaining five percent of global detections to hone in on more sophisticated attack phases.

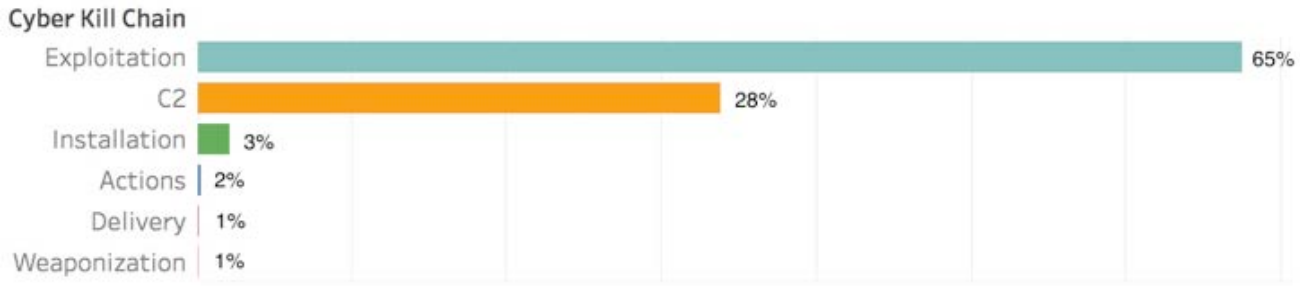

Figure 1: Cyber Kill Chain stages in descending order according to log count.

As shown in Figure 1, after removing reconnaissance, the exploitation phase accounted for 65 percent of remaining detections. Exploitation is the third stage of the Cyber Kill Chain in which the threat actor has completed reconnaissance, weaponized their tools or payloads, and successfully delivers the exploit to the intended target.

The business services industry accounted for 86 percent of all events correlated to the exploitation phase of the Cyber Kill Chain. Buffer overflows were attackers' primary focus throughout the month of July. This prompted the GTIC to analyze buffer overflow vulnerabilities in support of this report.

Of note, NTT Security covered the Lockheed Martin Cyber Kill Chain in great detail in the 2016 Global Threat Intelligence Report (GTIR).

2 Buffer Overflow Vulnerabilities

Analyzing network traffic flagged for possible buffer overflow attempts against the target showed the two most popular vulnerabilities leveraged by attackers were CVE-2017-7269 and CVE-2017-2934. Although both vulnerabilities are relatively new, exploit attempts against CVE-2017-2934 are not surprising, as they result in a heap-based buffer overflow in Adobe Flash Player. Attackers regularly leverage heap-based buffer overflow vulnerabilities in conjunction with exploit kits and phishing emails. Heap-based buffer overflows are commonly used for malware installation or to conduct arbitrary code execution after exploitation.

CVE-2017-7269 is a vulnerability in the WebDAV services as part of Internet Information Services (IIS) 6.0 in Microsoft Windows Server 2003 R2, support for which was stopped approximately two years ago. Successful exploitation allows the actor to remotely execute code on the targeted host. Based on the

description provided by NIST, the exploit is possible by using a customized HTTP PROPFIND request with a long header beginning with *"If: <http://"*. A plugin for Metasploit is available, increasing the ease of exploitation.

CVE-2017-7269 Information:
CVSS v3 Base Score: 9.8 Critical
Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H (legend)
Impact Score: 5.9
Exploitability Score: 3.9
CVSS Version 3 Metrics:

- Attack Vector (AV): Network
- Attack Complexity (AC): Low
- Privileges Required (PR): None
- User Interaction (UI): None
- Scope (S): Unchanged
- Confidentiality (C): High
- Integrity (I): High
- Availability (A): High

GTIC - Threat Research identified over 525,000 hosts vulnerable to this CVE based on a simple Shodan scan and strongly advises that you patch this vulnerability or upgrade to a supported version.

3 Vulnerability of the Month

Multiple Oracle Vulnerabilities

Threat Status: Critical

Severity: **Critical** (CVSS: 10.0)

Date: July 19, 2017

Remediation Details: Update to the latest software version

Affected Versions:

- Refer to the Affected Products and Components list.

Analyst Note: Oracle released a quarterly Critical Patch Update, ***addressing over 300 vulnerabilities.*** The vulnerabilities are spread over 90 Oracle products. This is the largest ever Quarterly Critical Patch Update for Oracle, with many of the vulnerabilities rated as ***Critical*** and over half of the vulnerabilities remotely exploitable.

All associated vulnerabilities should be evaluated and patched based on the risk they pose to your network. As an example, one of the vulnerabilities addressed in this patch was CVE-2017-10244, which allowed attackers to view potentially sensitive documents from the Oracle E-Business Suite without authentication.

4 Worldwide Hacking Campaign Targeting Energy/Critical Infrastructure

Researchers have identified a wave of phishing emails in a global campaign targeting critical infrastructure and energy companies. The campaign is thought to have begun in 2015, targeting companies in the Middle East and Western Europe.

The current wave of emails, which began in May 2017, attempts to steal user credentials by getting the user to download a template file from an attacker-controlled server after the user opens an infected MS Word document, which typically appears to be a résumé or environmental report. These emails were delivered primarily to critical infrastructure and energy companies, predominantly in Europe and the United States.

This malware variant was only detected by about a third of anti-virus software solutions.

The fact that this global campaign is designed to harvest user credentials and conduct reconnaissance is telling. It appears these attacks are not intended to cause damage – at least not at this phase of the campaign. Attacks of this type may indicate potential future attacks or may be used to maintain a foothold in a network for other reasons, such as acquiring access to intelligence or intellectual property (IP) over time.

The FBI and DHS issued a joint alert, warning energy companies that unnamed foreign hackers were attempting to steal login and password information so attackers could hack into networks. The alert also suggested that attacks have, so far, focused on employees' computers but have not affected control systems networks. There is no evidence to date that any information on operations has been exposed.

Although attribution has not been officially placed, many researchers believe that Russian threat actors may be involved, and that these types of attacks will likely continue.

Though nation-state actors like Russia have greater funding and capabilities, regardless of attribution, the targeting of these industries is concerning, as it shows a concentrated and timely effort to compromise U.S., European and Middle Eastern energy markets.

These types of campaigns illustrate that phishing campaigns aren’t simply spam emails, but rather are targeted, focused and aggressive, and are likely being carried out as part of a longer-term strategy.

On a related note, it also appears that the motivations for attacks are shifting to “cyber-disruptive” operations, possibly meant to influence an organization or sector in one way or another, meaning that

nation-state attackers could attempt to influence a targeted country by undermining confidence in its national infrastructure.

U.S. officials have conceded that many key systems which run critical infrastructure processes within the U.S. were not designed with strong security in mind. In addition, U.S. and industry officials have acknowledged that this was the first time hackers associated with the Russian government are known to have targeted U.S. power companies.

Many of these attacks have remained undetected since 2015, and mitigation efforts are often reactive rather than preemptive. NTT Security recommends keeping patches up to date, maintaining awareness of the threat to infrastructure and IP, and understanding that enterprise networks hold an incredible amount of value to attackers.

References:

Energy sector hacking campaign targeted more than 15 U.S. firms

Energy, Nuclear Targeted with Template Injection Attacks

5 GDPR: Why It Matters

The General Data Protection Regulation (GDPR), set to go into effect on May 25, 2018, is not optional.

If your organization maintains *any* data on people who live in the European Union (E.U.), you must comply.

Garry Sidaway, senior vice president of security strategy and alliances for NTT Security put it this way: "While the GDPR is a European data-protection initiative, the impact will be felt right across the world for anyone who collects or retains personally identifiable data from any individual in Europe."

The GDPR is unique in that it stipulates a maximum fine of four percent of the offending organization's annual turnover or 20 million euros (around $23 million USD), whichever is the greater of the two.

The GDPR becomes increasingly problematic for organizations who maintain personally identifiable information **(including emails)** of leads, prospects and clients. The regulation requires that if that data is collected and maintained, it must be maintained in that person's home country.

If your organization has not yet begun preparations for GDPR compliance, there is less than a year for you to do so. Read more about understanding the GDPR here.