

# Attacks Against the Government Sector

By Threat Hunter Team

## Table of Contents

Introduction

Examples of Attacks

Ransomware

Espionage

Denial of Service

Who is Attacking?

Iran

China

Russia

North Korea

Malicious Activity Trends

Ransomware

Network-Based Activity

Attack Tactics, Techniques,  
and Procedures

Case Studies

Case Study 1 - Legitimate  
Executables Abused to Side-load  
Malicious DLLs

Case Study 2 - Early Access to  
Unpatched Microsoft Exchange  
Server Vulnerabilities

Conclusion

Protection

Mitigation

Appendix A: Indicators of  
Compromise (IOCs)

Appendix B: DLL Search Order  
Hijacking Mitigation



## Introduction

The government sector, both U.S. and international, is a prime target for hackers. Attacks from organized criminals, foreign countries, political hacktivists, and others not only erode public trust in targeted government entities, but can also seriously impact government operations and the ability to deliver critical functions—not to mention the financial cost and risk to sensitive information and vital infrastructure. This all means that cyber security is a large and growing concern for governments worldwide.

Increasingly, federal, state, and local governments are targets as threat actors attempt to steal or manipulate sensitive data or disrupt operations. This was highlighted in December 2020 when news emerged of the [SolarWinds supply chain attack](#) in which multiple parts of the U.S. Federal Government, NATO, the UK government, and the European Parliament were impacted. The incident, which also impacted thousands of organizations in the private sector, was reported to be among the worst cyber-espionage incidents ever suffered by the U.S.

Different types of groups or individuals can initiate attacks against the government sector, and their motivations vary widely. Foreign nations may seek to obtain sensitive information about government operations; criminals may steal government employee data to hold for ransom or to sell and commit fraud; and hacktivists motivated by ideology rather than profit may seek to disrupt or gather information to further their agenda. In addition, types of attack can also vary widely, ranging from ransomware, to email-based social engineering attacks, to zero-day exploits, and supply chain attacks.

### What is the Government Sector?

As the government sector is vast and incorporates a wide range of entities, for this paper we chose to use the Public Administration sector as defined by the North American Industry Classification System (NAICS). **Sector 92: Public Administration** is defined as consisting of establishments of federal, state, and local government agencies that administer, oversee, and manage public programs and have executive, legislative, or judicial authority over other institutions within a given area.

Some of the key areas covered in this paper include the following:

- **Examples of Attacks:** Some recent examples of attacks against government entities broken up into common attack types/motivations.
- **Who is Attacking?** A look at some prominent advanced persistent threat (APT) groups with a focus on targeting the government sector.
- **Malicious Activity Trends:** Key trends taken from Symantec, a division of Broadcom (NASDAQ: AVGO), metrics.
- **Case Studies:** A detailed look at two cases worked on by the Symantec Threat Hunter Team.
- **How to Protect Your Network:** Protection and mitigation information that can be used by organizations in the government sector to protect their networks.

## Examples of Attacks

While cyber attacks against the government sector are far too numerous to list, in recent times there have been a number of notable incidents that highlight the range of attacks this sector is subject to, as well as the various tactics employed.

### Ransomware

#### Argentinian Border Crossing Shut Down

In August 2020, **Argentina's immigration agency (Dirección Nacional de Migraciones)** suffered a ransomware attack that forced it to close the country's border crossing. The Netwalker ransomware (Ransom.Netwalker), also known as Mailto, infected a number of servers at the immigration agency, which led to it deciding to completely shut down networks used by immigration offices and control posts. This meant that border crossings were suspended for several hours. The malware operators initially demanded a \$2 million ransom, however, this increased to \$4 million after the Argentinian government refused to negotiate with the criminals.

#### Ireland's National Health Service

On May 14, 2021, Ireland's national health service, the Health Service Executive (HSE), was **hit with a ransomware attack** that led to it having to shut down its IT systems. The attack impacted all its national and local services.

The attack was committed by a suspected Russian cyber crime group using the Conti ransomware (Ransom.Conti). The threat actors claimed they had access to the HSE network for two weeks, stole 700 GB of unencrypted files, and demanded a \$20 million ransom. The Irish government said it would not be paying any ransom. Shortly after this announcement, the Conti attackers **provided a free decryptor** but warned they would still publish stolen patient data online unless a ransom was paid.

Ireland's Department of Health (the parent department of the HSE) was also **targeted by the Conti gang**. The department shut down its systems following the incident but Ireland's Minister for Communications said that the attack "wasn't as extensive" as the HSE attack and was intercepted earlier.

## Espionage

### SolarWinds Supply Chain Attack

In mid-December 2020, news broke of the SolarWinds supply chain attack. In this particular case, rather than attacking the targets directly, the hackers compromised a third-party software provider (SolarWinds), accessing its build system and sneaking malicious code into updates to popular software Orion.

By compromising the update mechanism for SolarWinds' Orion software, the attackers were able to deliver a backdoor Trojan known as Sunburst (Backdoor.Sunburst). While thousands of organizations downloaded the Trojanized software update, the attackers were only interested in a relatively small selection. The nature of supply chain attacks mean they are indiscriminate, with any user of the compromised software at risk of infection. The attackers then get to pick and choose from the infected organizations, focusing on high-value targets for, in this case, the purpose of espionage.

A number of key U.S. federal agencies downloaded the malicious update, including the Department of Commerce, the Department of Homeland Security, the Treasury Department, and the Justice Department. The Justice Department later revealed that around **3% of its Office 365 mailboxes had been accessed by the attackers behind the attack**. NATO, the UK government, and the European Parliament were also impacted by the SolarWinds attack.

In April 2021, three months after news first broke of the attack, the U.S. government said that SVR, the Russian Foreign Intelligence Service (aka Fritillary, APT 29, Cozy Bear) **was responsible for the SolarWinds attack**. The U.S. imposed wide-ranging sanctions against Russia as a response.

Symantec carried out extensive research into the SolarWinds attack, including detailed analysis of additional malware (**Teardrop** and **Raindrop**) used by the attackers and insights into the command and control process used. All this research, along with protection information, can be found **on our dedicated blog page**.

### Dragonfly Exploiting Known Vulnerabilities

In October 2020, the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) released a **joint statement** revealing attacks carried out by a Russian state-sponsored hacking group against U.S. government networks. The hacking group was **Dragonfly** (aka Energetic Bear, Berserk Bear, Crouching Yeti, Koala).

The attackers had been targeting dozens of state and local government networks since at least February 2020. The group successfully compromised network infrastructure and exfiltrated data from at least two victim servers by combining exploits for known VPN appliances and Windows vulnerabilities. The hackers used the vulnerabilities to breach networking gear, pivot to internal networks, elevate privileges, and steal sensitive data.

Targeted devices included Citrix access gateways (**CVE-2019-19781**), Microsoft Exchange email servers (**CVE-2020-0688**), Exim mail agents (**CVE 2019-10149**), and Fortinet SSL VPNs (**CVE-2018-13379**). To move laterally across compromised networks, the attackers used the Zerologon elevation-of-privilege vulnerability in Windows Servers (**CVE-2020-1472**) to access and steal Windows Active Directory (AD) credentials.

## Denial of Service

### Belgian Government Knocked Offline by DDoS Attack

In May 2021, **Belgium's government was hit with a major distributed denial of service (DDoS) attack** that knocked most of its network offline, including public-facing websites and internal systems. The attack targeted Belnet, a state-owned ISP that provides connectivity and infrastructure for the country's government and public sector organizations. At least 200 public organizations were affected by the attack, including the country's tax portal, remote learning systems used by schools, and its COVID vaccine registration portal.

While the attack has yet to be attributed to anyone, several Belgian politicians and political observers suggested that the incident may have been politically motivated.

## Who is Attacking?

As well as ransomware actors out for financial gain and hacktivists with a goal of making political statements, advanced persistent threat (APT) groups are one of the biggest threats to the government sector. These highly skilled and typically state-sponsored threat actors are well resourced and use sophisticated hacking techniques to gain access to target networks. Because of the level of effort needed to carry out these attacks, APTs are usually leveled at high-value targets, such as those in the government sector.

The following selection of advanced persistent threat (APT) groups have been known to target the government sector. Each APT group is listed under the nation state it is believed to receive direction and support from.

### Iran

#### Crambus

Believed to have been active since at least 2014, Crambus (aka APT34, Oilrig, Twisted Kitten) is known to have targeted government agencies, financial institutions, and technology companies in Saudi Arabia, Israel, the United Arab Emirates (UAE), Lebanon, Kuwait, Qatar, the U.S., and Turkey.

The group delivers a custom backdoor known as Heherminth via spear-phishing attacks, targeting individuals within organizations of interest using malicious Office documents with embedded macros to install a backdoor. The group may also send emails containing links to websites registered by the attackers and employ social-engineering tactics to trick victims into downloading and installing the backdoor.

The goal of the group is cyber espionage, focusing on reconnaissance efforts to benefit Iranian nation-state interests.

### China

#### Cicada

The Chinese government-linked group known as Cicada (aka APT10, Stone Panda, Cloud Hopper) has been active since at least 2009 and is believed to be involved in espionage-type operations. Cicada traditionally customizes publicly available malware in concert with dual-use tools during operations. The group leverages a number of techniques during the initial stages of attack, such as targeted email, strategic website compromise, and supply chain attacks.

Cicada is known to target numerous sectors, including government, aerospace, energy, engineering, financial, healthcare, IT, manufacturing, media, and research. The group is known to target the following regions: Australia, China, Hong Kong, Japan, Taiwan, the UK, and the U.S. However, since 2016, Cicada appears to have mainly focused on targeting organizations in Japan across numerous sectors, including government, media, research, and transport. In November 2020, Symantec uncovered evidence that Cicada was behind a [large-scale attack campaign targeting multiple Japanese companies](#), including subsidiaries located in as many as 17 regions around the globe in a likely intelligence-gathering operation.

Cicada is known to use a combination of generally available malware and tools during operations, including the following:

- Backdoor.Darkmoon (Specific configurations)
- Backdoor.ChChes (Exclusively used)
- Backdoor.Korplug (Specific configurations)
- Trojan.Redleavy (Exclusively used)
- Trojan.Wimhop (A modified version of wmiexec.vbs available on GitHub)
- Backdoor.Hartip
- Tcping (Publically available tool to check connectivity)
- Csvde (Microsoft tool for Active Directory)
- PsExec (Microsoft tool for executing commands/files on a remote host)
- Netsess (Publically available tool to enumerate NetBIOS sessions)
- Trojan.Agentemis (aka Cobalt Strike)

## Budworm

Budworm (aka APT27, Lucky Mouse, Emissary Panda) has been active since at least July 2013.

The Chinese government-linked group uses the malware families Backdoor.Korplug, Trojan.Browrat, and Hyperbro in its attacks. Budworm has been known to leverage strategic website compromises and spear-phishing attacks to target victims in the aerospace, defense, government, and technology industries.

According to ESET, in early 2021 Budworm began exploiting several [Microsoft Exchange Server zero-day vulnerabilities](#). The group targeted multiple government networks in the Middle East and wider organizations in Central Asia for the purpose of cyber espionage. The group used the email server access, and the compromise of Microsoft SharePoint, to deploy a newly updated modular toolkit known as SysUpdate, which is designed to provide on-demand malicious capabilities.

## Russia

### Swallowtail

Swallowtail (aka APT28, Sofacy, Fancy Bear, Tsar Team, Sednit) is believed to be a Russian cyber espionage group that has been active since at least January 2007. The group was initially known for traditional, information-stealing espionage campaigns, targeting governments in the U.S. and Europe. It became involved in more overt, disruptive operations in the run-up to the 2016 U.S. presidential election.

The group has been known to employ a variety of methods to gain access to targeted organizations' networks. These include spear-phishing emails, watering hole websites, infected storage devices, and exploitation of software vulnerabilities, including zero-day vulnerabilities.

During the 2016 U.S. presidential election attacks, APT28 used spear-phishing emails that tricked recipients into supposedly changing their email passwords on a fake webmail domain. The group then used these stolen credentials to gain access to email accounts and steal the contents. This information was later leaked.

Symantec has seen APT28 use a number of custom malware tools, including:

- Infostealer.Sofacy
- OSX.Sofacy
- Trojan.Sofacy
- Trojan.Modruner

In December 2020, the Norwegian police secret service (PST) stated that it believed Swallowtail was likely responsible for [hacking the email accounts of the Norwegian Parliament](#) (Stortinget). In the attack, which took place in August 2020, the hackers gained access to the Parliament's email system and accessed inboxes for Stortinget employees and elected officials.

### Fritillary

Fritillary (aka APT29, Cozy Bear, the Dukes) is believed to be a Russian cyber espionage group and has been active since at least January 2010. Like APT28, it initially confined itself to spying campaigns, focusing on governments, the military, and think tanks in the U.S. and Europe. It later became involved in more subversive operations and was implicated (along with APT28) in disruptive attacks prior to the 2016 U.S. presidential election.

APT29 usually relies on spear-phishing emails to gain access to targeted organizations' networks. During the 2016 U.S. presidential election attacks, APT29 sent spear-phishing emails to more than 1,000 targeted individuals, including some U.S. government personnel. These emails contained malicious links which, if clicked, would lead to malware being installed on the target's computer. This allowed APT29 to compromise a political party's systems and steal emails from several accounts on the network.

Symantec has seen APT29 use a number of custom malware tools, including:

- Trojan.Cozer
- Trojan.Seaduke
- Trojan.Dionisduke
- Backdoor.Netduke
- Trojan.Powerduke
- Backdoor.Miniduke

More recently, the Federal Bureau of Investigation (FBI), the U.S. Department of Homeland Security (DHS), and the Cybersecurity and Infrastructure Security Agency (CISA) warned of [continued attacks coordinated by the Russian Foreign Intelligence Service](#) (SVR) (aka Fritillary) against U.S. and foreign organizations. The agencies said this activity, which included the SolarWinds Orion supply chain compromise (see Examples of Attacks), primarily targets government networks, think tank and policy analysis organizations, and information technology companies and seeks to gather intelligence information.

For more information on the Swallowtail and Fritillary groups, read our blog [Subverting Democracy: How Cyber Attackers Try to Hack the Vote](#).

## North Korea

### Springtail

Springtail (aka Kimsuky, Thallium, Nickle Foxcroft) has been active since at least 2012. The group is believed to be [operating on behalf of the North Korean government](#).

Springtail uses the malware families Trojan.Destfallen, Trojan.Kisuky, and Bloodhound.hwp.5 in its attacks. The group is known to use social engineering tactics, spear-phishing emails, and watering hole attacks to compromise its victims in order to gain intelligence on various topics of interest to the North Korean government.

Springtail targets individuals and organizations in South Korea, Japan, and the U.S. Springtail specifically targets individuals identified as experts in various fields, think tanks, and South Korean government entities. The group focuses its intelligence collection activities on foreign policy and national security issues related to the Korean peninsula, nuclear policy, and sanctions.

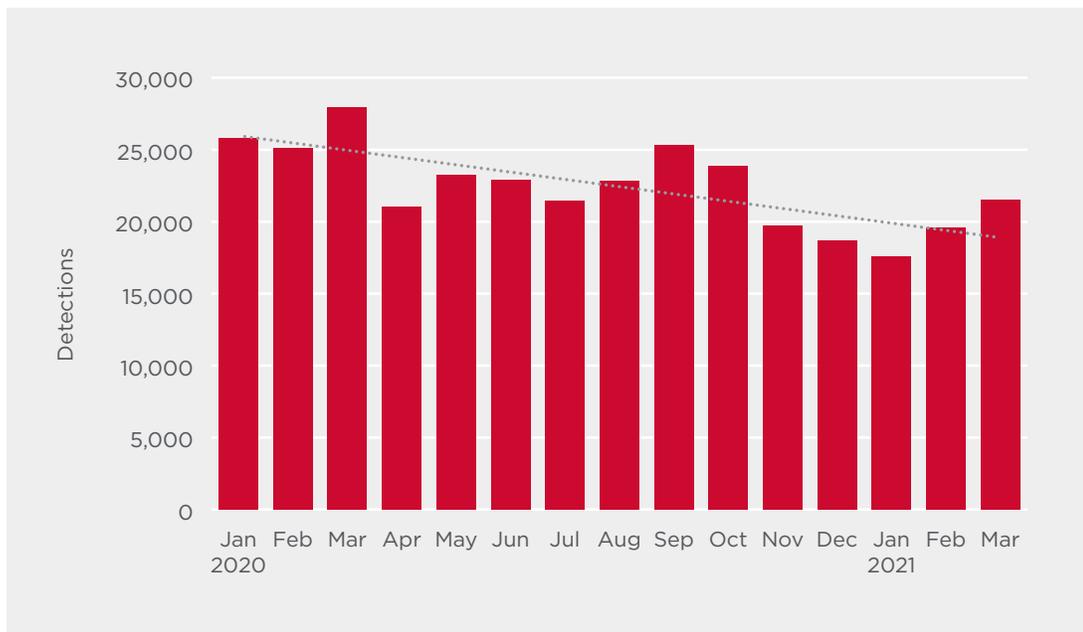
In September 2020 it was reported that Springtail attempted to [hack 11 officials of the United Nations Security Council](#).

In November 2020, Cybereason identified a new modular spyware suite dubbed KGH\_SPY and a new malware strain dubbed CSPY Downloader being **employed in attacks by Springtail**. The group was observed targeting a wide array of victim organizations in the U.S., Europe, Japan, South Korea, and Russia. The target organizations included pharmaceutical and research companies working on COVID-19 therapies, government and defense organizations, journalists, and various human rights groups.

## Malicious Activity Trends

In order to assess general levels of malicious activity, we examined telemetry from 1,100 government customers over the past 15 months, namely all of 2020 and the first quarter of 2021.

**Figure 1: Malware Detections by Month, January 2020 to April 2021**



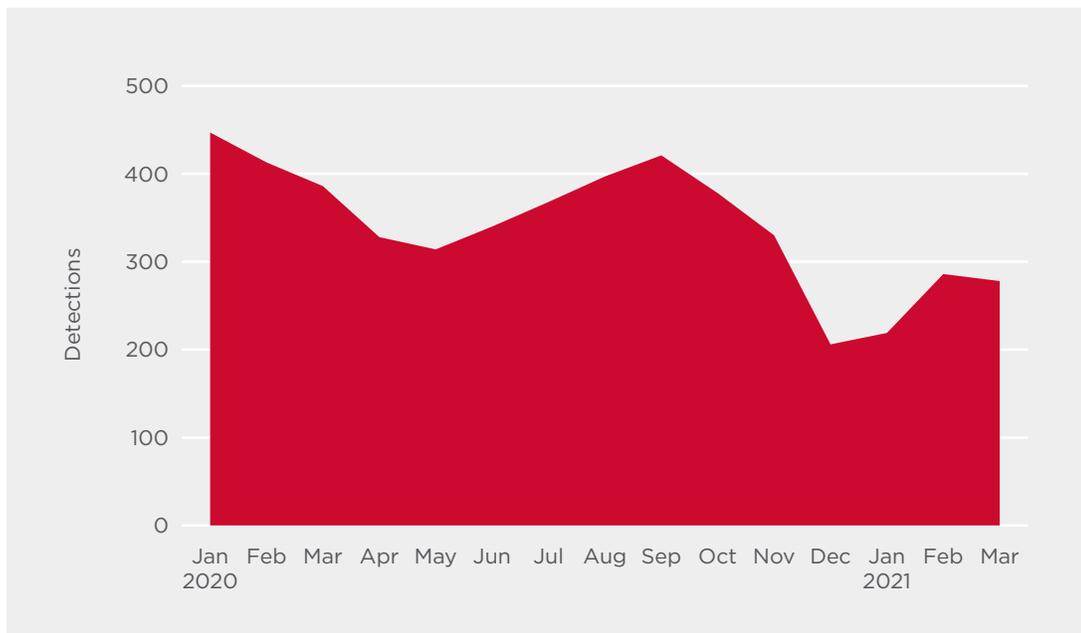
Malware detections in these organizations trended downwards in this time period. While the trend is welcome news, it shouldn't be cause for complacency since the decline was relatively small. Secondly, the biggest sources of risk to government organizations—espionage and ransomware—tend to be low prevalence but high impact threats.

## Ransomware

While the number of ransomware detections is showing a downward trend, this can be misleading as the number of victims is still considerable and, due to changing tactics from ransomware operators, the impact from successful attacks can be devastating.

It should also be noted that the data shown in Figure 1 is only a representative sample of the overall number of attacks involving ransomware. Most targeted ransomware operators, for example, recompile their ransomware for every new attack. This means that the variant of the ransomware used in an attack may be blocked by a generic or machine learning-generated detection signature rather than a detection linked to that ransomware family.

Figure 2: Ransomware Detections for Government Sector, January 2020 to March 2021



While in the past attackers were content with encrypting a victim organization's files, now most of the leading ransomware operators are stealing data prior to encryption and using it to increase the pressure on victims to pay up. The threat actors threaten to release the stolen data or sell it to the highest bidder if the victim doesn't pay a ransom.

Some ransomware gangs that have carried out ransomware attacks employing these tactics include the following:

### Maze

The now-defunct Maze ransomware gang was the first ransomware gang to adopt the tactic of exfiltrating data from victim organizations prior to encryption and threatening to release this data unless the ransom is paid. Maze also operated as a ransomware-as-a-service (RaaS), providing the malware to affiliates and sharing a portion of profits made from successful attacks.

In September 2020, Maze targeted Fairfax County Public Schools (FCPS). The school was just one of the U.S. public sector organizations hit by Maze since it first appeared in May 2019. Maze published 100 MB of data in an effort to pressure FCPS into paying a ransom. The ransomware gang said that the data represented just 2% of the total amount stolen during the attack.

Maze shut down operation shortly after the FCPS attack, with many of its affiliates at the time moving to the newly emerging Egregor RaaS.

### Babuk

In April 2021, the Babuk ransomware gang targeted Washington DC's Police Department and posted screenshots of some of the 250 GB of data it allegedly stole. The screenshots published by Babuk appeared to contain folders relating to police operations, DC gangs, and police disciplinary records. Babuk even claimed to have files relating to arrests following the storming of the U.S. Capitol building on January 6.

Just two weeks later, Babuk released what it claimed was another 22 GB of data belonging to the police department following the breakdown of ransom negotiations. The gang published the data on its dedicated data leak website. According to reports, the Babuk operators were initially seeking a \$4 million ransom. According to the screenshots posted by Babuk, the police department offered \$100,000, but this wasn't acceptable to the ransomware gang. The additional leaked data allegedly included arrest files, financial files, case files, disciplinary files, and more.

A relatively new arrival to the ransomware scene, Babuk first appeared in January 2021. The ransomware gang targets victims in human-operated attacks. While Babuk initially used the strong Elliptic-curve Diffie-Hellman algorithm to encrypt files, the ransomware gang has since claimed that it will no longer be encrypting victims' data and will instead solely focus on data theft and extortion.

### Ryuk and Conti

In October 2020, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) issued a warning about an increase in Emotet attacks against state and local government organizations. The Emotet Trojan was originally designed to steal banking credentials from an infected computer and also add it to a botnet. However, Emotet developed into a major distribution channel for other malware families, including targeted ransomware threats such as Ryuk and Conti.

Ryuk and Conti, along with the GoGalocker and MegaCortex ransomware families, are controlled by a single adversary that Symantec calls Miner. The ransomware threats operate on a ransomware-as-a-service (RaaS) business model, with the creators sharing the ransomware with affiliated attackers in exchange for a cut of the ransom.

In all of Miner's ransomware operations, the threat actors use Cobalt Strike, which runs in the memory of infected computers, making detection difficult. Cobalt Strike is used by Miner to download additional tools and to create a reverse shell providing the attackers with additional access.

Miner was likely leasing access to Emotet from the botnet's operators and using that access to target its victims with Ryuk. Ryuk was previously distributed by the Trickbot botnet.

However, in early 2021, law enforcement agencies announced they had taken control of the Emotet botnet's infrastructure, which they used to deliver an update that removed the malware from infected computers.

This did not spell the end for Miner, though, which also relies on malicious spam campaigns, and compromising exposed RDP connections to gain access to victim networks, mounting brute force and password spraying attacks against RDP.

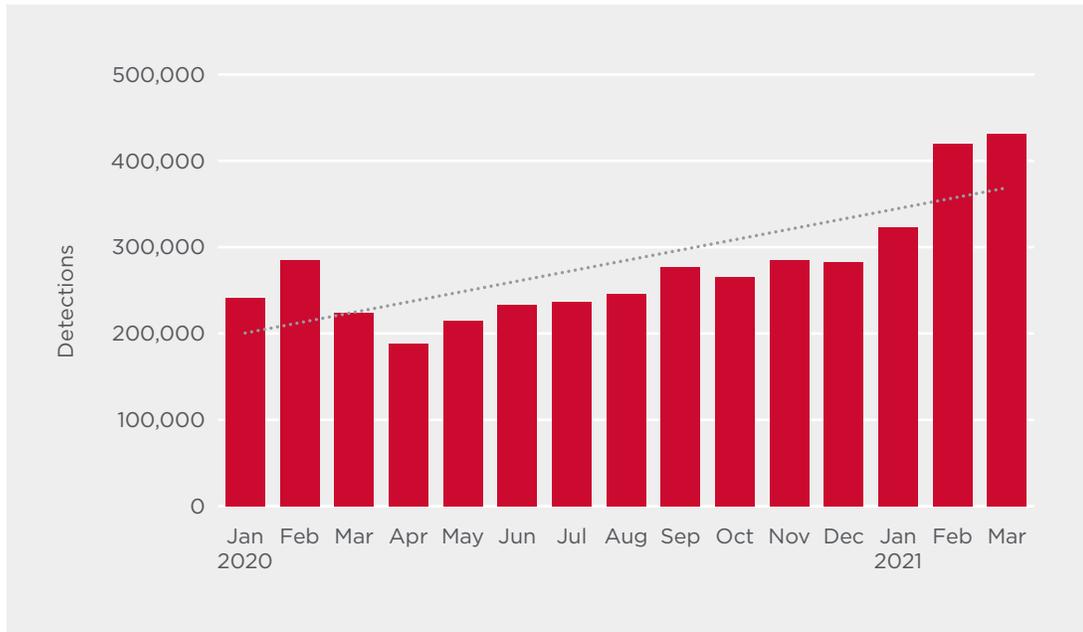
In August 2020, Conti joined the list of targeted ransomware families to create a public data leak website in order to increase the pressure on victims to pay a ransom. Conti is believed to have strong links to Ryuk. While Ryuk was being distributed via the Trickbot botnet, in July 2020, the botnet stopped delivering Ryuk and begun delivering Conti instead.

The Conti ransomware recently made headlines when it infected Ireland's Health Service Executive (HSE), the country's national health service, demanding a \$20 million ransom for the return of stolen data.

### Network-Based Activity

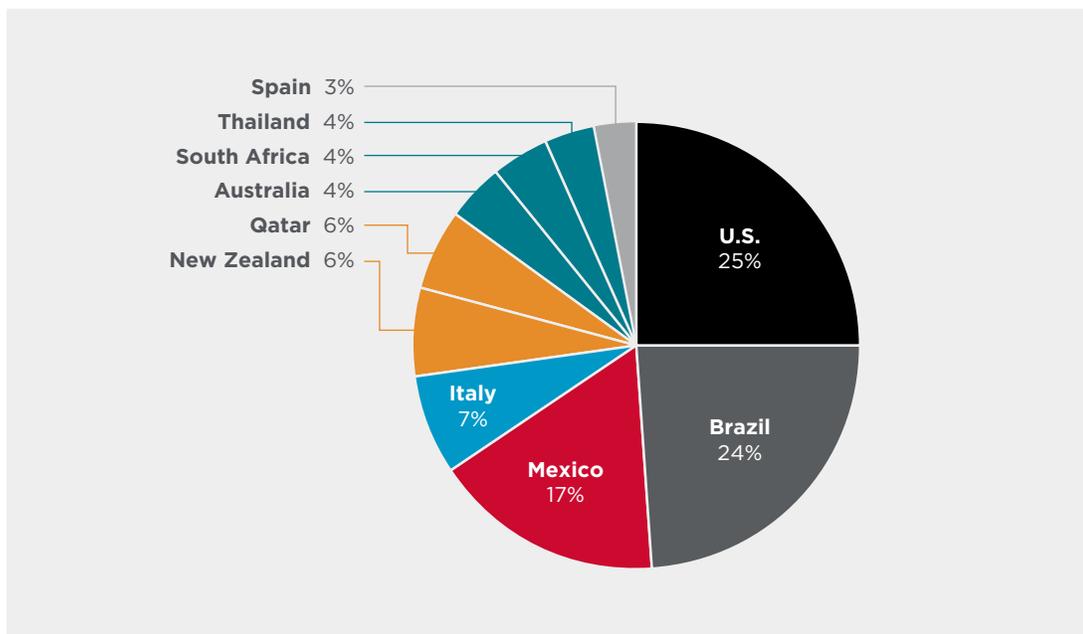
Malware detections form only one part of the picture, and more information can be gleaned from attacks blocked on the network by our Intrusion Prevention (IPS) technologies. Malicious network-based activity reveals more information about the extent of malicious activity on organizations' networks by blocking activity at the application layer. If a machine on a network becomes infected, the malware is likely to attempt to contact a command and control (C&C) server, which can also trigger these detections. Looking at the number of network detections attempting to contact a C&C server can give us a more realistic idea about how many infected machines are on a network and a truer picture of the extent of malicious activity in a sector.

Figure 3: IPS Detections, January 2020 to March 2021



IPS detections have trended upwards in the same time period, suggesting that while the number of confirmed malware infections fell slightly, the number of infection attempts has risen.

Figure 4: Top 10 Regions with a Government Sector Targeted by Malware in 2020



When looking at the countries where the government sector is most frequently targeted by malware, the U.S. is the most represented, accounting for nearly a quarter of all malware detections. This is unsurprising, since the U.S. is a populous country, with multiple layers of government at both federal and state level.

When it comes to countries targeted by malware the most, in addition to the U.S. we often see China, the UK, and France in the top 10, countries that didn't make the list here. The fact that Brazil and Mexico take second and third place here indicates that the government sector in these countries is of significant interest to attackers.

With regard to the other countries in the top 10, there are few surprises, many being large states with federal government structures.

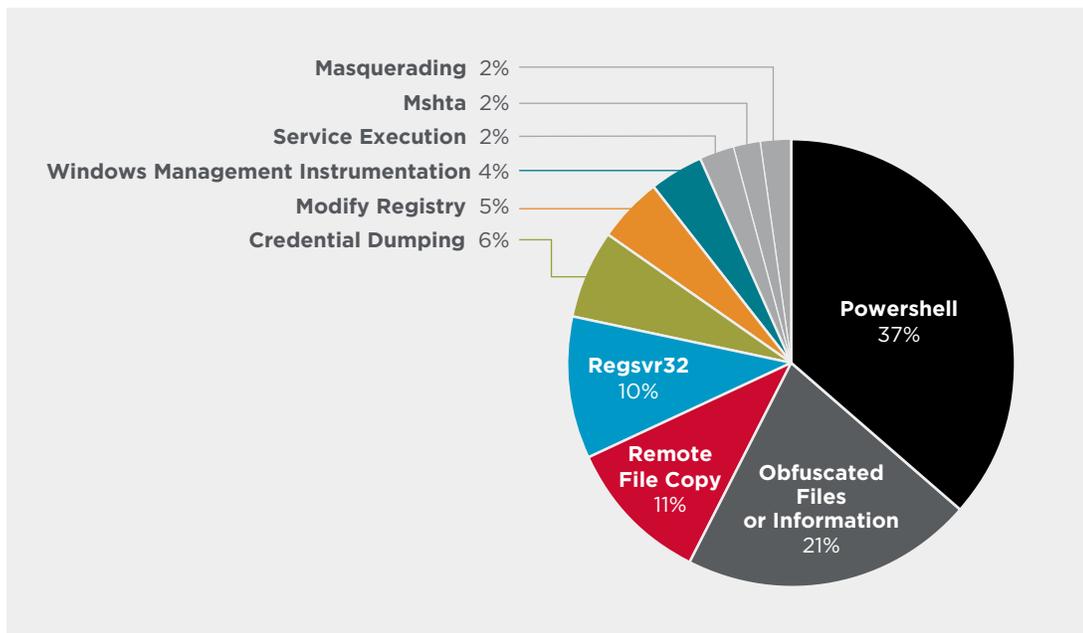
## Attack Tactics, Techniques, and Procedures

The MITRE ATT&CK® matrix classifies attack techniques and tactics. It divides attack tactics into the following 12 main categories, which map to the typical attack chain between vector and payload execution:

- **Initial Access**
- **Execution**
- **Persistence**
- **Privilege Escalation**
- **Defense Evasion**
- **Credential Access**
- **Discovery**
- **Lateral Movement**
- **Collection**
- **Command and Control**
- **Exfiltration**
- **Impact**

Within these categories, there are 245 distinct attack techniques. Some may be employed at multiple stages of an attack chain, meaning they can apply to more than one of the above 12 categories. Symantec Cloud Analytics classifies all incidents with a MITRE technique name. With millions of incidents logged each year, it is possible to form a picture of the most frequently used techniques. Cloud Analytics draws on intelligence gathered from analyst investigations and leverages advanced machine learning to identify and block patterns of suspicious activity. Because it is designed to identify malicious activity, more so than malicious tools, the vast majority of incidents created relate to living-off-the-land tactics.

Figure 5: Top MITRE Techniques Used in Attacks Against the Government Sector in 2020



The following are some of the most common Mitre ATT&CK techniques used by threat actors targeting the government sector in 2020:

- **PowerShell:** PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system. It can be abused to perform a number of actions, including discovery of information and execution of code.
- **Obfuscated Files or Information:** Attempting to make a malicious file difficult to discover by encoding it or otherwise obfuscating its contents.
- **Remote File Copy:** Transferring tools or files from external sources onto a compromised network, either via download from a command and control (C&C) server or through other methods such as FTP.
- **Regsvr32:** Regsvr32.exe is a command-line program used to register and unregister object linking and embedding controls. Attackers may abuse Regsvr32.exe for proxy execution of malicious code.
- **Credential Dumping:** Obtaining credentials, either hashed or in clear text, usually through a dump of the computer's memory. A range of freely available tools such as Mimikatz or LaZagne can be used to perform this task.
- **Modify Registry:** Modifying the registry to hide configuration information within registry keys, or deleting information in order to remove evidence of intrusions.
- **Windows Management Instrumentation (WMI):** Microsoft command-line tool, which can be used to execute commands on remote computers.
- **Service Execution:** The Windows service control manager (services.exe) is an interface to manage and manipulate services. It can be used to execute malicious commands or payloads.
- **Mshhta:** Mshta.exe is a Microsoft utility that executes HTML Application (HTA) files. Attackers may abuse mshta.exe for proxy execution of malicious .hta files and JavaScript or VBScript through a trusted Windows utility.
- **Masquerading:** Manipulating files and tools in order to make them appear to be legitimate or benign in order to evade detection.

## Case Studies

The following two case studies are examples of some of the more recent investigations carried out by the Symantec Threat Hunter Team. The incidents, which both impacted organizations in the government sector, offer a snapshot into what these organizations are targeted by and highlight a small selection of the methods used by the attackers.

### Case Study 1 - Legitimate Executables Abused to Side-load Malicious DLLs

In April 2021, Symantec technology identified a number of suspicious files on multiple computers on the networks of two government agencies, one in a Southeast Asian country and another in a country in South Asia. The investigation found that the attackers were abusing legitimate executables for side-loading malicious DLLs in order to execute a backdoor threat (RDoorBackdoor) on victim computers.

The motive for the attacks appears to have been information gathering. In one case, the attackers appeared to be targeting information related to the Association of Southeast Asian Nations (ASEAN).

RDoorBackdoor has been in use since at least 2018. It appears to be used in targeted attacks only but it is unclear if the backdoor is a shared tool or exclusive to one attack group. The attack activity discussed in this case occurred between June 2020 and April 2021.

While the initial infection vector is unknown, the lead up to the final payload begins with RDoorDropper, a self-extracting (SFX) RAR file. RDoorDropper contains three files:

- A legitimate and signed PE vulnerable to DLL search-order hijacking
- A malicious loader (RDoorLoader)
- An encrypted .pak file containing the final payload (RDoorBackdoor)

We observed RDoorDropper variants abusing PEs for four different legitimate applications and a **discontinued plug-in** for Internet Explorer:

**Table 1: Legitimate PEs Abused by the Attackers**

Legitimate binary	Loader (RDoorLoader)	Encrypted payload (RDoorBackdoor)
SiteAdv.exe (McAfee SiteAdvisor)	SiteAdv.dll	SiteAdv.pak
ssr32.exe (Sophos SafeStore Restore)	safestore32.dll	safestore.pak
wsc_proxy.exe (Avast wsc_proxy)	wsc.dll	proxycfg.pak
colnst.exe (Norton Identity Safe)	msvcr100.dll	coinstcfg.dat
chrome_frame_helper.exe (Google Chrome Frame)	chrome_frame_helper.dll	chrome_frame_helper.pak

When opened, RDoorDropper extracts the embedded files and executes the legitimate PE in order to load RDoorLoader, which is side-loaded via search order hijacking by the legitimate PE.

### What is DLL search order hijacking?

Dynamic link library (DLL) side-loading via search order hijacking is a cyber attack method that takes advantage of how Microsoft Windows programs handle DLL files. In DLL search order hijacking attacks, malware places a spoofed malicious DLL file in a specific Windows directory so that the operating system loads it instead of the legitimate file.

Windows allows programs to load DLLs at runtime and programs can specify the location of DLLs to load by specifying a full path, using DLL redirection, or by using a manifest. If none of these methods are used, Windows tries to locate the DLL by searching a list of directories in a set order.

Attackers abuse this search feature by placing a malicious DLL in one of those directories. Often this is the current working directory of the program. Then Windows finds and loads the malicious DLL before the legitimate version.

It is also possible to execute code within the context of a legitimate portable executable (PE) by abusing insecure library references. If a developer allows LoadLibrary to resolve the path of a library dynamically then that PE will also look in the current directory for the library DLL.

A threat actor can copy a legitimate PE to a directory where the attacker has write access. If the attacker creates a custom payload DLL, the program will load that DLL and execute the malicious code. This can be beneficial for the attacker as the PE may be signed and appear trustworthy to some security solutions, and it may also bypass application white listing (AWL).

## Post compromise

### RDoorBackdoor

RDoorBackdoor is a fully featured backdoor with the ability to install itself as a service, log keystrokes, communicate with its command and control server (C&C) using HTTP, HTTPS, DNS, UDP, or TCP, and listen on a local port for commands.

Instances of RDoorBackdoor are usually identical with the exception of embedded and encrypted configuration which determines:

- C&C communication method
- Service details
- Installation directory

The attackers using RDoorBackdoor used a number of non-malware techniques for credential theft:

- PowerShell was used to launch rundll32.exe in order to dump the memory of a process using the MiniDump function of comsvcs.dll (this is a technique used often to dump LSASS memory)
- Reg.exe was used to dump the SAM and SYSTEM registry hives
- A legitimate Avast tool was used by the attackers to dump LSASS memory

Other post-compromise tools used by the attackers included:

### LSASS dumping tool

- The only credential theft tool found to be used by the attackers
- Similar to how PowerShell is used, this tool can dump LSASS process memory using the legitimate comsvcs.dll file

### BrowsingHistoryView

- A utility that reads the history data of different web browsers

### Chrome secrets stealer

- A Chrome secrets and history stealer based on <https://github.com/LimerBoy/Adamantium-Thief/tree/master/Stealer/Stealer>

### NirCmd

- Small command-line utility for carrying out various tasks without a user interface

### Suspected NirCMD

- Found disguised with a similar name to other suspicious files

### Command-line downloader

- This downloader can be passed proxy information and a remote host and will attempt to download and execute a DLL file

### Forfiles

- Dual-use tool that searches files according to the specified search mask and runs a specified command on each item found
- Used by the attackers to search for a specific file name

Multiple machines where RDoorBackdoor was observed also had additional malware and tools present, including the following:

- **GupdataLoader:** A simple loader that reads and executes shellcode from a separate file named favico.ico.
- **ChromeDecryptor:** Chrome secrets and history stealer based on the [LimerBoy/Adamantium-Thief](#) stealer.
- **NightScoutBackdoor and NightScoutDropper:** Malware previously [described by ESET](#) (Malicious Update variant 1).
- **PrcLoader:** A loader for the aPLib compressed executable stored in the Windows Registry (HKEY\_CLASSES\_ROOT\prc\Shell).
- **GrouperLoader:** A service-based loader for shellcode stored in the Windows Registry. Shellcode is encrypted using the computer name as a key.
- **UpdateRootkitDropper:** A dropper for embedded rootkit drivers (32-bit & 64-bit) and backdoor payloads stored in a separate file (res.dat). The dropper contains code consistent with previously seen instances of ZXShell that also included rootkit capabilities. Extracted rootkit drivers are tagged as UpdateRootkit. Several instances of droppers for UpdateRootkitDropper were also observed (UpdateRootkitDropperDropper). Final payloads stored in a separate file (res.dat) are likely instances of ZXShell.
- **DosEmulator and FastProxy:** Tools previously [described by Trend Micro](#) that are part of the Korplug/PlugX build and control toolset.

## Case Study 2 - Early Access to Unpatched Microsoft Exchange Server Vulnerabilities

---

Snail (aka Calypso) are believed to be in operation since 2016. First publicized in October 2019, the group is believed to be of Asian origin and is involved in espionage-type operations on a global scale. Snail are known to exploit publicly facing applications to install their malware. The group can be identified by the use of a custom malware called Calypso RAT (Trojan.Calypso).

The group has been observed targeting organizations in various sectors including the government, as well as electronics, IT, and transport.

Once they have compromised a network, Snail are known to deploy web shells and the custom Calypso RAT malware. Additionally, Snail have reportedly leveraged open-source tools such as network and port scanners and tunneling tools. The group has also leveraged exploit tools such as EternalBlue, DoublePulsar, and EternalRomance.

Organizations in the following regions have been targeted by Snail:

- Afghanistan
- China
- India
- Japan
- South Korea
- U.S.

Snail are known to target public-facing applications in order to initially compromise victims. In 2020, Snail reportedly had early access to an unpatched Microsoft Exchange Server vulnerability chain ([ProxyLogon](#)) in order to deploy their malware.

ProxyLogon is a pre-authentication remote code execution (RCE) vulnerability chain (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065) that can allow an attacker to take over any reachable Exchange server, without the need for valid account credentials.

Before Microsoft released out-of-band patches for vulnerable versions of Exchange server on March 2, 2021, a number of APT groups, which included Snail, had already been [exploiting ProxyLogon in the wild](#). This means that the threat groups did not reverse engineer the Microsoft updates, as is often the case. However, it is unclear how the groups gained access to the details of the vulnerabilities before the release of the patches.

On March 1, 2020, a full day before Microsoft released patches, Snail used the ProxyLogon vulnerabilities to compromise the email servers of government entities in the Middle East and in South America. In the following days, the group used the exploit to target additional servers of government entities and private companies in Africa, Asia, and Europe.

The group deployed a web shell, the Calypso RAT malware, and a custom backdoor. The malicious tools are loaded using DLL search-order hijacking (see Case Study 1) against legitimate executables also dropped by the group.

## Conclusion

While cyber security is a challenge for every sector, those in the government sector are being targeted by a range of threat actors whose capabilities and persistence continue to grow. The government sector forms the backbone of civil service and, as such, a cyber attack against it can have dire consequences. This threat should not be overlooked and organizations must take the necessary steps and precautions to bolster their defensive capabilities to prevent them from falling prey to a cyber attack or data breach, and the people they serve from losing out on key services.

## Protection: How Symantec Solutions Can Help

The Symantec Enterprise Business provides a comprehensive portfolio of security solutions to address today's security challenges and protect data and digital infrastructure from multifaceted threats. These solutions include core capabilities designed to help organizations prevent and detect advanced attacks.

### **Symantec Endpoint Security Complete**

Symantec Endpoint Security Complete (SESC) was specifically created to help protect against advanced attacks. While many vendors offer EDR to help find intrusions, as does Symantec, there are gaps. We call these gaps blind spots and there are technologies in SESC to eliminate them.

[Learn More](#)

### **Privileged Access Management (PAM)**

PAM is designed to prevent security breaches by protecting sensitive administrative credentials, controlling privileged user access, proactively enforcing security policies and monitoring and recording privileged user activity.

[Learn More](#)

### **Symantec Web Isolation**

Symantec Web Isolation eliminates web threats and solves the challenge of providing access to unknown, uncategorized and potentially risky web sites by creating a remote execution environment between an agency's enterprise systems and content servers on the web.

[Learn More](#)

### **Symantec Secure Web Gateway (SWG)**

SWG delivers high-performance on-premises or cloud secure web gateway that organizations can leverage to control or block access to unknown, uncategorized, or high-risk web sites.

[Learn More](#)

### **Symantec Intelligence Services**

Symantec Intelligence Services leverages the Symantec Global Intelligence Network to deliver real-time threat intelligence to several Symantec network security solutions including Symantec Secure Web Gateway, Symantec Content Analysis, Symantec Security Analytics, and more.

[Learn More](#)

### **Symantec Content Analysis with Advanced Sandboxing**

Within the Symantec Content Analysis platform, zero-day threats are automatically escalated and brokered to Symantec Malware Analysis with dynamic sandboxing for deep inspection and behavioral analysis of potential APT files and toolkits.

[Learn More](#)

### **Symantec Security Analytics**

Symantec Security Analytics delivers enriched, full-packet capture for full network traffic analysis, advanced network forensics, anomaly detection, and real-time content inspection for all network traffic to arm incident responders for quick resolution.

[Learn More](#)

## Mitigation

Symantec security experts recommend users observe the following best practices to protect against targeted attacks.

### Local Environment:

- Monitor the use of dual-use tools inside your network.
- Ensure you have the latest version of PowerShell and you have logging enabled.
- Restrict access to RDP Services. Only allow RDP from specific known IP addresses and ensure you are using multi-factor authentication (MFA).
- Implement proper audit and control of administrative account usage. You could also implement one-time credentials for administrative work to help prevent theft and misuse of admin credentials.
- Create profiles of usage for admin tools. Many of these tools are used by attackers to move laterally undetected through a network.
- Use application allow lists where applicable.
- Locking down PowerShell can increase security, for example with the constrained language mode.
- Make credential dumping more difficult, for example by enabling credential guard in Windows 10 or disabling SeDebugPrivilege.
- MFA can help limit the usefulness of compromised credentials.

### Email:

- Enable MFA to prevent the compromise of credentials during phishing attacks.
- Harden security architecture around email systems to minimize the amount of spam that reaches end-user inboxes and ensure you are following best practices for your email system, including the use of SPF and other defensive measures against phishing attacks.

## Appendix A: Indicators of Compromise (IOCs)

### Case Study 1 - Legitimate Executables Abused to Side-load Malicious DLLs

#### Rdoor Related

SHA256	Description
02d9dd1e5ba9219b4e4355cdaa03bec4c8f1f51987fd1fd0c1f874d8080289d9	RDoorDropper
fb4a37d889c3464a77435263e8d34a8dd230a46c55b7898c759551dd67b8c1b1	RDoorDropper
eb095d26af3b46574b27f1b3607e7a18de7605ffa453697e19e379ca0e814df6	RDoorDropper
3e2ace7c603cd2ea80621cf67bb6a4b3ae3da2ffda32e0634a6056362cb58321	RDoorDropper
adbc72273d87ae5f507c34a9ab5146d7a3df66d04910488c42277af47e105578	RDoorDropper
b09a936b948ec1196d4346f1f99f4ccc528e9bfec66b2da3c8c108fe0188c5f0	RDoorDropper
3a89606cd9549dd15726948181dad1725ab7b89d6b07623f4087325bc03b9371	RDoorDropper
0317fc04275e70014f70934701bc75023d843d67b582b6cc03fcf6c2d736db17	RDoorDropper
1d6453e34951a4201d9b65275d2bc48354b1596486b1018d4ac4bd7cb96e081a	RDoorDropper
3dfb118bdcf2e9af07f26a6ca0636c574442bcce3b5a14e1fcb44ca975ad766	RDoorLoader
fd5a032e0e00b9ebf7703a83d608928cb2539e5794ecaadd44089a86b6ac4d25	RDoorLoader
1892716a335e73082f183a44c9769374b240e503658d2d2a7cc4c46ef7f3ffc6	RDoorLoader
fa5f32457d0ac4ec0a7e69464b57144c257a55e6367ff9410cf7d77ac5b20949	RDoorLoader
8317246b19lead7adf148a43fcf3f9f49897125fff89fcc8ebf5333c07d83aa1	RDoorLoader
1cce581820c55c2c46dd6140bc420891f4237f481264fedcc27e7d426858540	RDoorLoader
084f5a29f60e183a6244bbcfa41565294adfd6503f695b65b3d89c763a69cc83	RDoorLoader

#### Legitimate Applications Abused for Malware Loading

SHA256	Description
1ab4f52ff4e4f3aa992a77d0d36d52e796999d6fca1a109b9ae092a5d7492b7dd	Google Chrome Frame
eb3b4e82ddfdb118d700a853587c9589c93879f62f576e104a62bdaa5a338d7b	McAfee SiteAdvisor
8b6352ef7e0b70db156691ae16aa52f245141f62e2661f54532f3832cad732de	Avast remediation tool
fb42e8ddb4a9ca87f292d68b4dc3d53fae6ddf2137f6c5bc7ad7d5ae1edf6b	Avast remediation tool
83f40e70ea3ba0e614d08f1070dafa75092660003b8a1f8b563d4f5b012f4bae	Kaspersky setup
3124fcb79da0bdf9d0d1995e37b06f7929d83c1c4b60e38c104743be71170efe	McAfee OEM module
59f6a21bb31fbfe4909945567f0ede3b34685cde78f5a72aea3074a677c8f5b1	Sophos SafeStore restore tool

#### Post-Compromise Tools

SHA256	Description
41a248b6b8df4a81845bcd10e4bb5e1eb3583a8d396f66a87b41d95c25d250c	Command line DLL downloader
67ebc03e4fbf1854a403ea1a3c6d9b19fd9dc2ae24c7048aafbbff76f1bea675	Loader
f92cac1121271c2e55b34d4e493cb64cdb0d4626ee30dc77016eb7021bf63414	Loader
6e4d5950f1419ae3922f135ec7be66be599f60e63458358f39ad684643cb6fa1	Scanner capable of scanning and fingerprinting multiple network services. Can also be used to discover default Tomcat credentials.

SHA256	Description
3bd0835c6d07d4ced6f76563bb0e183291a952cd2756af891d37f903df0fdab5	Unknown msi.dll likely to be executed by Kaspersky application
7751626d7a9469b942f62bcf7d35ce220de028a5aa27432f96f3d5ac1460a01d	Chrome secrets stealer
41d174514ed71267aaff578340ff83ef00dbb07cb644d2b1302a18aa1ca5d2d0	LSASS dumping tool
e94a5bd23da1c6b4b8aec43314d4e5346178abe0584a43fa4a204f4a3f7464b9	Reconnaissance tool
ace18b3bdac31fb4d731377f3950d78db28b09896aa71224658b9d49de2e47d2	forfiles (dual-use)
a3520ea56b94ab812da853719374ce3354bb6e39611521782d328da5ed619fef	forfiles (dual-use)
3c8fca34b2568cfd9cf54809160468ee0e06c12e80f194519a3aea3b6ca166bd	NirCmd (dual-use)
f14fe846126b166136e38c2e080585ed155e4ec296115283e796c0c64383e9e2	BrowsingHistoryView (dual-use)
2f223daf4a6d4ff52d53c8f532a780760411f9168ba95cb9937b8ee11e4d9b75	Avast dump process tool (signed, clean)

### Unknown, Suspicious Files

SHA256	Description
fa7f9e6bf52ab4a412e17c755c949e112c33fd336bce0809f0feddbec6d14faa	(Sample unavailable)
6931c2e70c8d6ef623899343ea7d5bc257f744a1da9a79bca87819300e261562	(Sample unavailable)
b5af9d596f2f2e6ab2c54c1690f19ea78cd7f8cf969ce3b9ce84e10605128427	(Sample unavailable)
2248ccd69a7eef74bfb335599441dc49cdeae7f28bdf5464a645c6a2834a0de	(Sample unavailable)
0a07416d85dbf84d6ac81fc97044e0814e9d807a004ad19ddd99b915272c35cb	(Sample unavailable)
4d15e85620ec23109328798b84ad09a4cabd5ef09244c47cc72652ca250a8851	(Sample unavailable)
599a7a5bc043c92f35191d4cd6fc3d34d7b8adc0be7a3f78877ba045c21eb0a6	(Sample unavailable)
7bd059f545e52e7bab4ceea96eaac51c658289507960baa13fcd5f43f91ff83e	(Sample unavailable)
b1f7f00edd18da8d026c8c91b20a99e46223dbcef37f072248edf6821466cc65	(Sample unavailable)
75d09d8768365f9503a22a1b5465e2e9f65d8f36a9d9a2d2f6bc685c12ecf4f5	(Sample unavailable)
cd63f3283205da20eef2a2bed71cab6dd22c4f15b6236a3a021a5d23b823290e	(Sample unavailable)
1c3947422abd14346aff08bc17a1570738c7529a7bc5804eddf224886a37b238	(Sample unavailable)
f7b79afb95e9f61aa9f93782c099b2fba36172b9ba234c5f863cdded1369977e5	(Sample unavailable)

### Network

Value	Description	First seen	Last seen
91[.]229[.]77[.]43	In configuration for loader 67ebc03e4fbf1854a403ea1a3c6d9b19fd9dc2ae24c7048aafbbff76f1bea675 passed as remote host in command line to downloader tool 41a248b6b8df4a81845bcdff0e4bb5e1eb3583a8d396f66a87b41d95c25d250c	2020-07-29	2020-07-29

## Appendix B: DLL Search Order Hijacking Mitigation

The MITRE ATT&CK® matrix lists the following mitigations for preventing DLL side-loading attacks:

### M1047 Audit

Use auditing tools capable of detecting DLL search order hijacking opportunities on systems within an enterprise and correct them. Toolkits like the PowerSploit framework contain PowerUp modules that can be used to explore systems for DLL hijacking weaknesses.

Use the program sxstrace.exe that is included with Windows along with manual inspection to check manifest files for side-by-side problems in software.

### M1038 Execution Prevention

Adversaries may use new DLLs to execute this technique. Identify and block potentially malicious software executed through search order hijacking by using application control solutions capable of blocking DLLs loaded by legitimate software.

### M1044 Restrict Library Loading

Disallow loading of remote DLLs. This is included by default in Windows Server 2012+ and is available by patch for XP+ and Server 2003+.

Enable Safe DLL Search Mode to force search for system DLLs in directories with greater restrictions (e.g. %SYSTEMROOT%) to be used before local directory DLLs (e.g. a user's home directory).

The Safe DLL Search Mode can be enabled via Group Policy at Computer Configuration > [Policies] > Administrative Templates > MSS (Legacy): MSS: (SafeDllSearchMode) Enable Safe DLL search mode. The associated Windows Registry key for this is located at HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\SafeDllSearchMode

## Detection

Monitor file systems for moving, renaming, replacing, or modifying DLLs. Changes in the set of DLLs that are loaded by a process (compared with past behavior) that do not correlate with known software, patches, etc., are suspicious. Monitor DLLs loaded into a process and detect DLLs that have the same file name but abnormal paths. Modifications to or creation of .manifest and .local redirection files that do not correlate with software updates are suspicious.



For product information and a complete list of distributors, visit our website at: [broadcom.com](https://broadcom.com)

Copyright © 2021 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries. Broadcom, the pulse logo, Connecting everything, and Symantec are among the trademarks of Broadcom.

© 2015-2021, The MITRE Corporation. MITRE ATT&CK and ATT&CK are registered trademarks of The MITRE Corporation.

SES-GOVS-WP107 June 10, 2021