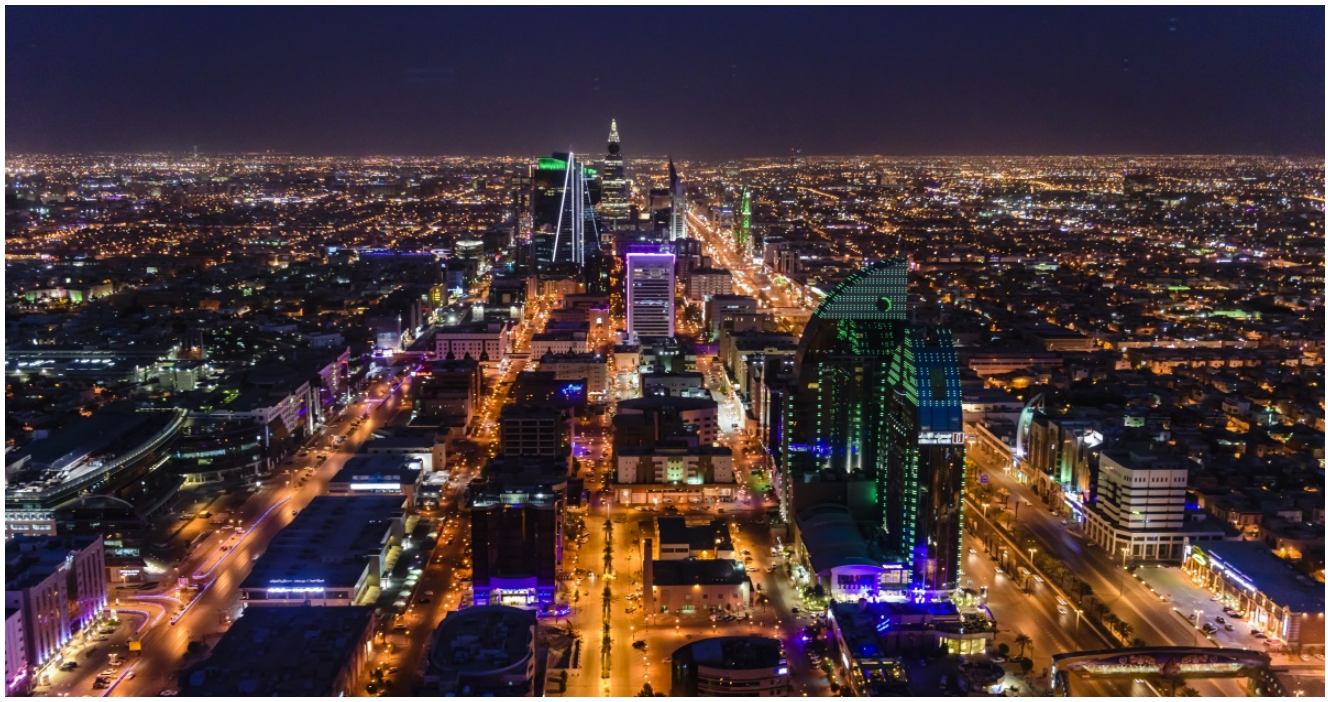
Tortoiseshell Group Targets IT Providers in Saudi Arabia in Probable Supply Chain Attacks

symantec.com/blogs/threat-intelligence/tortoiseshell-apt-supply-chain



Threat Hunter TeamSymantec

Previously undocumented group hits IT providers in the Middle East.

A previously undocumented attack group is using both custom and off-the-shelf malware to target IT providers in Saudi Arabia in what appear to be supply chain attacks with the end goal of compromising the IT providers' customers.

The group, which we are calling Tortoiseshell, has been active since at least July 2018. Symantec has identified a total of 11 organizations hit by the group, the majority of which are based in Saudi Arabia. In at least two organizations, evidence suggests that the attackers gained domain admin-level access.

"#Tortoiseshell group uses custom malware, off-the-shelf tools, #livingofftheland techniques to compromise victims https://symc.ly/2lV4Ovn"
Click to Tweet
Another notable element of this attack is that, on two of the compromised networks, several hundred computers were infected with malware. This is an unusually large number of computers to be compromised in a targeted attack. It is possible that the attackers were forced to infect many machines before finding those that were of most interest to them.

We have seen Tortoiseshell activity as recently as July 2019.

Custom tools

The unique component used by Tortoiseshell is a malware called Backdoor.Syskit. This is a basic backdoor that can download and execute additional tools and commands. The actors behind it have developed it in both Delphi and .NET.

Backdoor.Syskit is run with the "-install" parameter to install itself. There are a number of minor variations of the backdoor, but the primary functionality is the following:

- reads config file: %Windir%\temp\rconfig.xml
- writes Base64 encoding of AES encrypted (with key "fromhere") version of the data in the "url" element of the XML to:

HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\policies\system\Enablevmd

This contains the command and control (C&C) information.

writes Base64 encoding of AES encrypted (with key "fromhere") version of the "result" element of the XML to:

HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\policies\system\Sendvmd

This holds the later portion of the URL to append to the C&C for sending information to it.

deletes the config file

The malware collects and sends the machine's IP address, operating system name and version, and Mac address to the C&C server using the URL in the Sendvmd registry key mentioned above. Data sent to the C&C server is Base64 encoded.

The backdoor can receive various commands:

- "kill_me":
  stops the dllhost service and deletes %Windir%\temp\bak.exe
- "upload "
  downloads from the URL provided by the C&C server
- "unzip"
  uses PowerShell to unzip a specified file to a specified destination, or to run cmd.exe /c <received command>

Tools, techniques, and procedures

The other tools used by the group are public tools, and include:

- Infostealer/Sha.exe/Sha432.exe
- Infostealer/stereoversioncontrol.exe
- get-logon-history.ps1

Infostealer/stereoversioncontrol.exe downloads a RAR file, as well as the get-logon-history.ps1 tool. It runs several commands on the infected machine to gather information about it and also the Firefox data of all users of the machine. It then compresses this information before transferring it to a remote directory. Infostealer/Sha.exe/Sha432.exe operates in a similar manner, gathering information about the infected machine.

We also saw Tortoiseshell using other dumping tools and PowerShell backdoors.

The initial infection vector used by Tortoiseshell to get onto infected machines has not been confirmed, but it is possible that, in one instance, a web server was compromised to gain access by the attacker. For at least one victim, the first indication of malware on their network was a web shell (d9ac9c950e5495c9005b04843a40f01fa49d5fd49226cb5b03a055232ffc36f3). This indicates that the attackers likely compromised a web server, and then used this to deploy malware onto the network.

> This activity indicates the attackers had achieved domain admin level access on these networks, meaning they had access to all machines on the network.

Once on a victim computer, Tortoiseshell deploys several information gathering tools, like those mentioned above, and retrieves a range of information about the machine, such as IP configuration, running applications, system information, network connectivity etc.

On at least two victim networks, Tortoiseshell deployed its information gathering tools to the Netlogon folder on a domain controller. This results in the information gathering tools being executed automatically when a client computer logs into the domain. This activity indicates the attackers had achieved domain admin level access on these networks, meaning they had access to all machines on the network.

Presence of OilRig tools

In one victim organization, we also saw a tool called Poison Frog deployed one month prior to the Tortoiseshell tools. Poison Frog is a backdoor and a variant of a tool called BondUpdater, which was previously seen used in attacks on organizations in the Middle East. The tools were leaked on Telegram in April this year and are associated with the group known as APT34, aka Oilrig.

It is unclear if the same actor deployed both the Poison Frog tool and the Tortoiseshell tools, however, given the gap in time between the two sets of tools being used, and without further evidence, the current assumption is that the activity is unrelated. If that is the case, this activity demonstrates the interest from multiple attack groups in industries in this region. The Poison Frog tool also appears to have been leaked prior to deployment to this victim, so could be used by a group unrelated to APT34/Oilrig.

Attacker motives

The targeting of IT providers points strongly to these attacks being supply chain attacks, with the likely end goal being to gain access to the networks of some of the IT providers' customers. Supply chain attacks have been increasing in recent years, with a 78 percent increase in 2018, as we covered in ISTR 24. Supply chain attacks, which exploit third-party services and software to compromise a final target, take many forms, including hijacking software updates and injecting malicious code into legitimate software.

IT providers are an ideal target for attackers given their high level of access to their clients' computers. This access may give them the ability to send malicious software updates to target machines, and may even provide them with remote access to customer machines. This provides access to the victims' networks without having to compromise the networks themselves, which might not be possible if the intended victims have strong security infrastructure, and also reduces the risk of the attack being discovered. The targeting of a third-party service provider also makes it harder to pinpoint who the attackers' true intended targets were.

The customer profiles of the targeted IT companies are unknown, but Tortoiseshell is not the first group to target organizations in the Middle East, as we have covered in previous blogs. However, we currently have no evidence that would allow us to attribute Tortoiseshell's activity to any existing known group or nation state.

Protection/Mitigation

The following protections are also in place to protect customers against Tortoiseshell activity:

- Backdoor.Syskit

Indicators of Compromise

SHA256	Name
f71732f997c53fa45eef5c988697eb4aa62c8655d8f0be3268636fc23addd193	Backdoor.Syskit
02a3296238a3d127a2e517f4949d31914c15d96726fb4902322c065153b364b2	Backdoor.Syskit
07d123364d8d04e3fe0bfa4e0e23ddc7050ef039602ecd72baed70e6553c3ae4	Backdoor.Syskit

Backdoor.Syskit C&C servers
64.235.60.123
64.235.39.45

About the Author

Threat Hunter Team

Symantec

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

Want to comment on this post?