Leafminer: New Espionage Campaigns Targeting Middle Eastern Regions

By About the Author

Archived: 2026-04-02 11:03:41 UTC

Symantec has uncovered the operations of a threat actor named Leafminer that is targeting a broad list of government organizations and business verticals in various regions in the Middle East since at least early 2017. The group tends to adapt publicly available techniques and tools for their attacks and experiments with published proof-of-concept exploits. Leafminer attempts to infiltrate target networks through various means of intrusion: watering hole websites, vulnerability scans of network services on the internet, and brute-force/dictionary login attempts. The actor’s post-compromise toolkit suggests that the group is looking for email data, files, and database servers on compromised target systems.

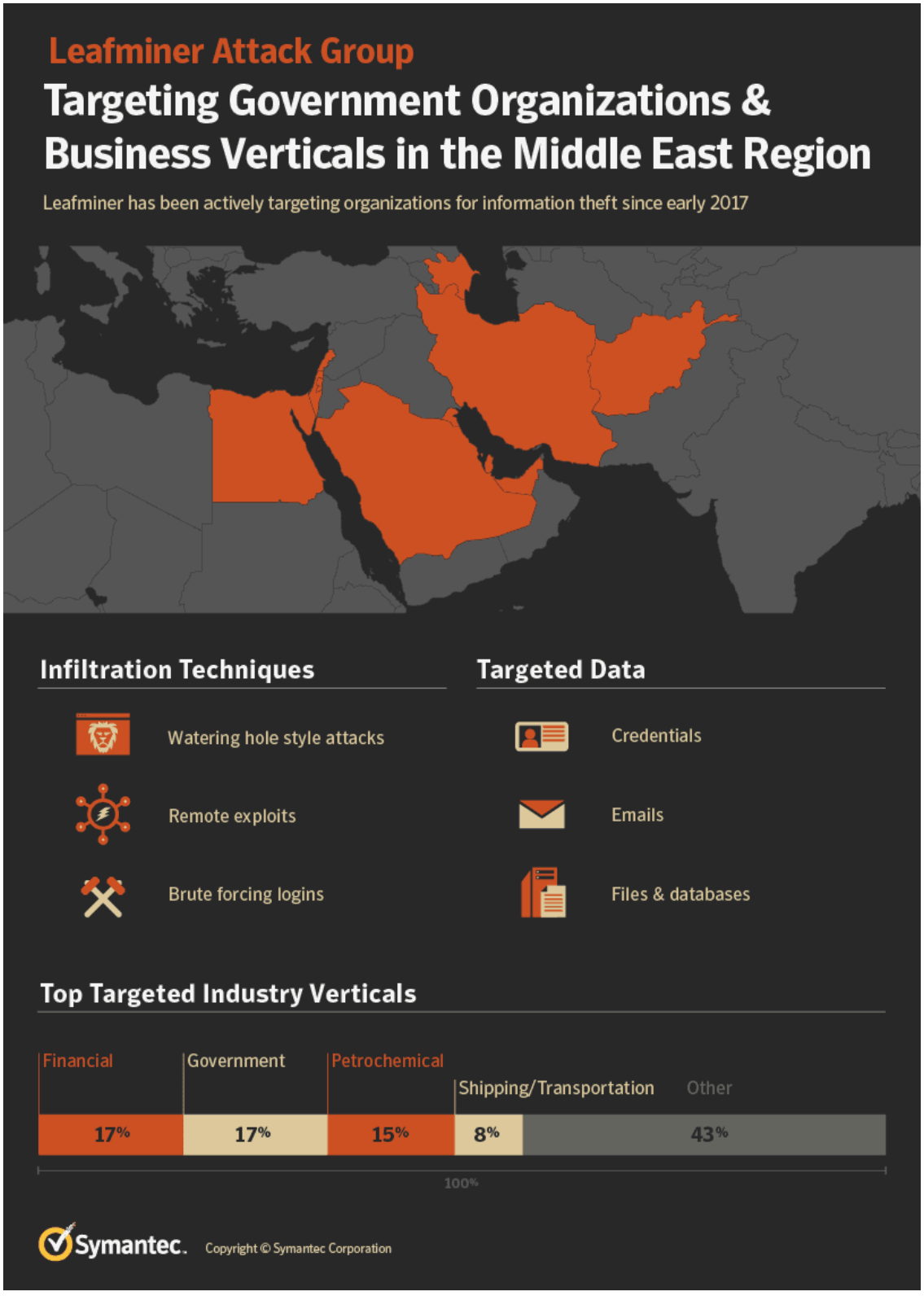

Figure 1. Leafminer targeting organizations in Middle East region

Leafminer's arsenal

During our investigation, there was a breakthrough discovery that helped connect Leafminer to a number of attacks observed on systems in the Middle East and identify the toolkit used in the group's efforts of intrusion, lateral movement, and exfiltration. The download URL for a malware payload used in one of the attacks lead to

the identification of a compromised web server on the domain e-qht.az that had been used to distribute Leafminer's arsenal of malware, payloads, and tools within the group and make them available for download from victim machines.

As of early June 2018, the server hosted 112 files in a subdirectory that could be accessed through a public web shell planted by the attackers. In addition to malware and tools, the served files also included uploads of log files seemingly originating from vulnerability scans and post-compromise tools.

The web shell is a modification of the PhpSpy backdoor and references the author MagicCoder while linking to the (deleted) domain magiccoder.ir. Researching the hacker handle MagicCoder results in references to the Iranian hacking forum Ashiyane as well as defacements by the Iranian hacker group Sun Army.

Targets

During the investigation of the Leafminer group, we were able to assemble a targeting profile from different sources including telemetry and log files hosted publicly on the attacker's arsenal server.

> One interesting source of target information discovered during the Leafminer investigation was a list of 809 targets used by the attackers for vulnerability scans.

Symantec detection telemetry shows malware and custom tools used by Leafminer on 44 systems across four regions in the Middle East.

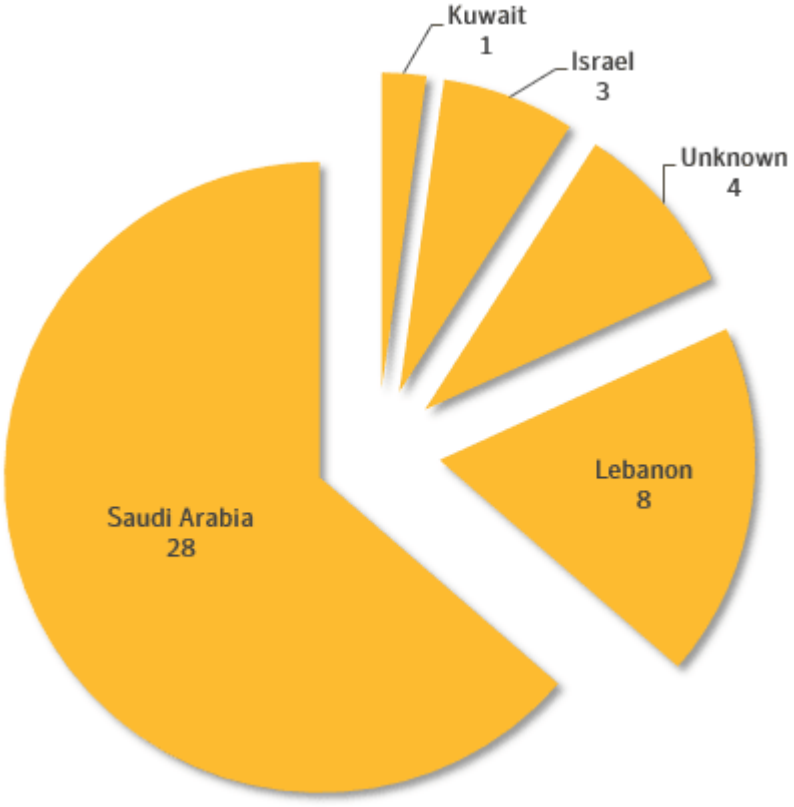

Figure 2. Infected computers per region

One interesting source of target information discovered during the Leafminer investigation was a list of 809 targets used by the attackers for vulnerability scans. The list is written in the Iranian language Farsi and groups each entry with organization of interest by geography and industry. Figure 3 shows a breakdown of the industry verticals. Targeted regions included in the list are Saudi Arabia, United Arab Emirates, Qatar, Kuwait, Bahrain, Egypt, Israel, and Afghanistan.

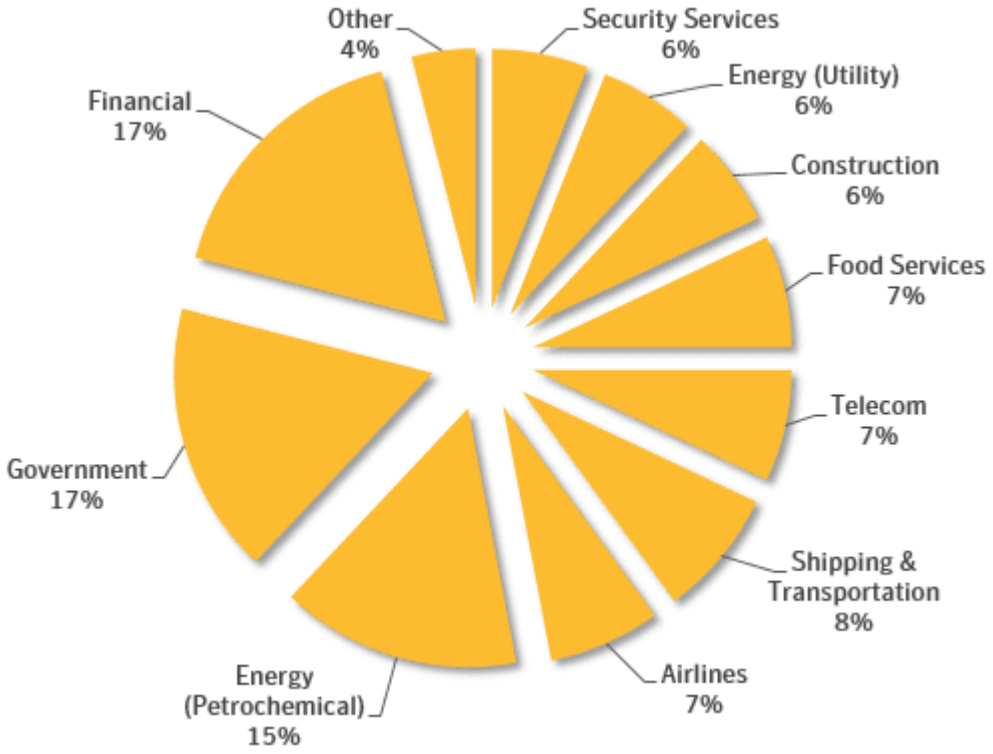

Figure 3. Industry verticals targeted by Leafminer

Intrusion

We observed three main techniques used by Leafminer for initial intrusion of target networks:

- Compromised web servers used for watering hole attacks
- Scans/exploits for vulnerabilities of network services
- Dictionary attacks against logins of network services

There are indicators that suggest the attackers have also employed email phishing with malicious attachment files. However, this was not directly observed or captured.

Watering hole SMB credential theft

Our investigation of Leafminer started with the discovery of JavaScript code on several compromised websites in the Middle East. The obfuscated code was planted by the attackers to steal SMB credential hashes that could subsequently be brute-forced offline.

When executing the code, the browser creates an invisible image tag and sets the URL to an attack server using the file:// protocol scheme. On Windows machines, this triggers a request to a remote server via the Samba

networking protocol (SMB) that also transmits the user's login NTLM hash. These hashes can be cracked to retrieve the original login password by methods of brute-force, dictionary, or rainbow table lookups.

Table 1 shows an overview of the compromised websites used as watering holes, infected JavaScript URLs, and SMB URLs used to collect NTLM hashes.

TLD	Region	Vertical	Infected JavaScript	SMB URL
gov.lb	Lebanon	Intelligence Agency	/assets/js/front/jquery.min.js	51.254.173.240/file.gif
org.sa	Saudi Arabia	Healthcare	/JavaScript/CommonJScript.js	adobe-plugin.bid/file.gif
edu.az	Azerbaijan	University	/_layouts/1033/init.js	188.165.187.235/file.gif

Table 1. Watering hole website details

Interestingly, the same technique was also observed in watering hole attacks by the threat actor Dragonfly in 2017 as reported by Symantec.

Vulnerability scans and exploitation

As previously mentioned, Leafminer seems to be actively following developments and publications of the offensive security community when selecting their toolkit. This became especially apparent when analyzing the group's techniques and tools for vulnerability scans and exploitation. The compromised web server used to store Leafminer's arsenal hosted several public proof-of-concept exploits and exploitation tools.

This included the Fuzzbunch framework that was part of an infamous leak of exploits and tools by the Shadow Brokers in April 2017. Leafminer has developed exploit payloads for this framework (Table 2) that deliver custom malware through attacks against SMB vulnerabilities described by Microsoft. The EternalBlue exploit from the framework received worldwide attention after being used in the ransomware campaigns WannaCry in May and Petya/NotPetya in June 2017. The Leafminer operators use EternalBlue to attempt lateral movement within target networks from compromised staging servers.

Symantec also observed attempts by Leafminer to scan for the Heartbleed vulnerability (CVE-2014-0160) from an attacker-controlled IP address. Furthermore, the Leafminer arsenal server hosted a Python script to scan for this vulnerability.

Dictionary attacks

Another intrusion approach used by Leafminer seems a lot less sophisticated than the previously described methods but can be just as effective: using specific hacktools to guess the login passwords for services exposed by a targeted system. This type of attack was observed both via dedicated servers set up by Leafminer as well as staging servers compromised by the group.

Commands found in a readme text that was stored in a ZIP archive together with the hacktool THC Hydra in Leafminer's tool arsenal represent online dictionary attacks on Microsoft Exchange and Remote Desktop Protocol

services of regional government servers in Saudi Arabia. "Online" in this case refers to the attacker using the protocol of the targeted network service to quickly run through many password guesses.

Custom malware

Symantec identified two strains of custom malware used by the Leafminer group: Trojan.Imecab and Backdoor.Sorgu. Directly connected to this malware are several sets of reflective loader DLLs used as droppers or to execute specific commands on a compromised system.

The development of custom malware by Leafminer as well as some of the tools used for lateral movement show a preference for the .NET framework. We also observed that the attackers would download and install the .NET framework on compromised machines, supposedly in the situation that an operator would have remote access to the system but required .NET to run Leafminer's custom tools. To this end, the command and control (C&C) server operated by the group hosted the legitimate setup executable for Microsoft .NET Framework 2.0 SP2.

Backdoor.Sorgu

Backdoor.Sorgu is used by the attackers to provide remote access to the infected machine. The backdoor is installed as a service in the Windows system through a shell command script.

Trojan.Imecab

The purpose of Trojan.Imecab is to set up a persistent remote access account on the target machine with a hardcoded password. Variants of the malware were also observed with the filename guester.exe which likely refers to the functionality of adding a powerful guest account to the system.

The malware installs itself in the system as a Windows service to achieve persistence and ensure that the guest account remains available to the attacker.

Reflective loader DLLs

Table 2 gives an overview of the reflective loader DLLs and their purpose:

File name	PDB string	Purpose
dnf2.x86.dll dnf2.x64.dll dnf4.x86.dll dnf4.x64.dll	…\Desktop\DLL\rat\code\dnf2\32\… …\Desktop\DLL\rat\code\dnf4\32\…	Drops & installs Backdoor.Sorgu
guester.x86.dll guester.x64.dll	…\Desktop\NSA\Payloads\guestsaz\32\…	Drops & installs Trojan.Imecab
remote.x86.dll remote.x64.dll	…\Desktop\NSA\Payloads\DLL\code\32\… …\Desktop\NSA\Payloads\DLL\code\32\x64\Release\…	Enables the Windows "Remote Desktop Protocol" service (RDP)
adm.add.x86.dll adm.add.x64.dll	…\Desktop\DLL\code\32\Release\… …\Desktop\shellcode\x64\Release\…	Creates/activates an admin user with a hardcoded password
vmware.x86.dll vmware.x64.dll	…\Desktop\ReflectiveDLLInjection-master\… …\Desktop\shellcode\x64\Release\…	Creates an admin user for Remote Desktop Protocol access

Table 2. Reflective loader DLLs

These DLLs were likely used as payloads for exploit shellcode of the Fuzzbunch framework, which is also evidenced by the embedded PDB strings.

Lateral movement and exfiltration

The discovery of malware and hacktools hosted on e-qht.az allowed us to correlate detection telemetry of potential Leafminer intrusions with tools made available for download to the group's operators. Understanding the purpose of the tools used by the attacker gives a unique insight into the tactics and procedures used by Leafminer after the initial compromise of a target network.

Table 3 outlines the observed toolset for lateral movement, information gathering, and exfiltration.

Software	Purpose	Description	Customized	Obfuscated
MSF Rotten Potato	Local	Privilege escalation		X
Mimikatz/OrangeTeghal	Lateral	Login/password retrieval	X	X
LaZagne	Lateral	Login/password retrieval		
THC Hydra	Lateral	Dictionary attacks against logins of network services		
Sysinternals PsExec	Lateral	Launch remote processes		
Total SMB BruteForcer	Lateral	Brute-force SMB logins	X	
Sysinternals PsInfo	Info	Get detailed information about remote systems		
Router Scan v2.47	Info	Scan for wireless networks		
MailSniper	Exfiltration	Search Exchange server mailboxes for keywords		
Sobolsoft Extract Attachments	Exfiltration	Extract attachments from EML email files		
SysTools SQL Backup Recovery	Exfiltration	Export backup of MSSQL databases		
HoboCopy	Exfiltration	Disk backup		
Voidtools Everything	Exfiltration	Desktop file indexing & search		

Table 3. Toolset for lateral movement, information gathering, and exfiltration

We discovered a number of servers compromised by Leafminer that were used as staging systems to gain a foothold in the targeted network and execute attacks on intranet resources. For example, the use of THC Hydra to execute dictionary attacks against Exchange logins was observed both in initial intrusion attempts as well as in lateral attacks from staging systems.

Figure 4 shows a screenshot of the Total SMB BruteForcer hacktool used by Leafminer for lateral movement. The tool requires input files with lists of IPs, users, and passwords respectively.

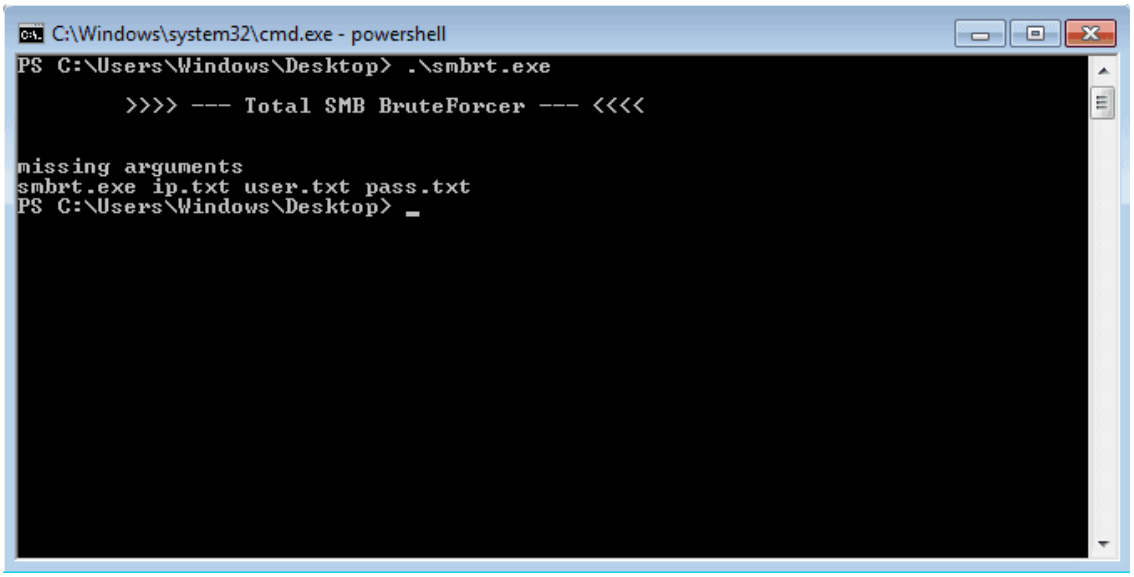

Figure 4. Total SMB BruteForcer

The arsenal server hosted five text files that could be used by Leafminer operators as input for dictionary attacks using Total SMB Bruteforcer and THC Hydra.

OrangeTeghal and Process Doppelgänging

One of the custom tools used by the Leafminer group is a rebranded version of the widespread post-exploitation tool Mimikatz.

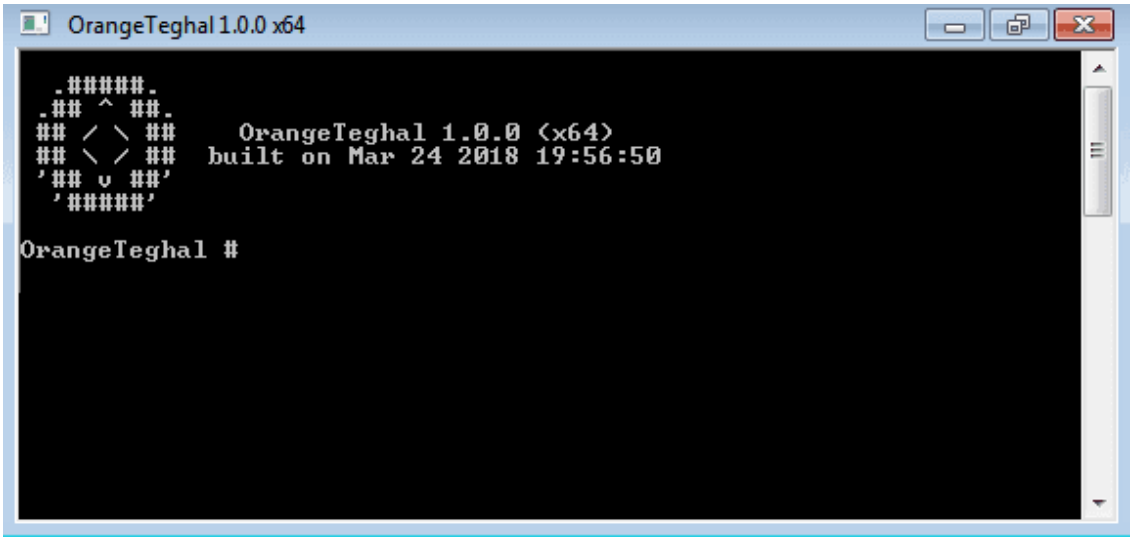

Figure 5. OrangeTeghal

While the logo and commands are identical to the original hacktool, the name was changed to OrangeTeghal. To evade security software while deploying this tool on compromised systems, the attackers use a technique revealed at Black Hat EU ‘17 in the presentation *Lost in Transaction: Process Doppelgänging*. The malware file orange64.exe is a .NET executable that drops and executes a PowerShell script with basic obfuscation. After deobfuscation, this script closely resembles the code published by the authors of the technique. Process

Doppelgänging uses NTFS transactions to modify the executable of a seemingly benign process that is suspended right after creation.

Ambitions blunted by inexperience

Leafminer is a highly active group, responsible for targeting a range of organizations across the Middle East. The group appears to be based in Iran and seems to be eager to learn from and capitalize on tools and techniques used by more advanced threat actors.

On a broad level, it has followed the recent trend among targeted attack groups for "living off the land"—using a mixture of publicly available tools alongside its own custom malware. More specifically, it mimicked Dragonfly's use of a watering hole to harvest network credentials. It also capitalized on the Shadow Brokers release of Inception Framework tools, making use of the leaked Fuzzbunch framework by developing its own exploit payloads for it.

> Leafminer's eagerness to learn from others suggests some inexperience on the part of the attackers, a conclusion that's supported by the group's poor operational security.

Leafminer has also been tracking developments in the world of cyber security. After the Heartbleed bug was disclosed it began scanning for instances of the vulnerability. It also utilized Process Doppelgänging, a detection evasion technique first discussed at the Black Hat EU conference last year.

However, Leafminer's eagerness to learn from others suggests some inexperience on the part of the attackers, a conclusion that's supported by the group's poor operational security. It made a major blunder in leaving a staging server publicly accessible, exposing the group's entire arsenal of tools. That one misstep provided us with a valuable trove of intelligence to help us better defend our customers against further Leafminer attacks.

Protection

Symantec has the following protections in place to protect customers against Leafminer attacks:

File-based protection

- Backdoor.Sorgu
- Trojan.Imecab

Threat intelligence

Customers of the DeepSight Intelligence Managed Adversary and Threat Intelligence (MATI) service have received intelligence that details the characteristics of the Leafminer cyber espionage group and methods of detecting and thwarting activities of this adversary.

Best Practices

- Important passwords, such as those with high privileges, should be at least 8-10 characters long (and preferably longer) and include a mixture of letters and numbers. Encourage users to avoid reusing the same

passwords on multiple websites and sharing passwords with others should be forbidden. Delete unused credentials and profiles and limit the number of administrative-level profiles created. Employ two-factor authentication (such as Symantec VIP) to provide an additional layer of security, preventing any stolen credentials from being used by attackers.

- Emphasize multiple, overlapping, and mutually supportive defensive systems to guard against single point failures in any specific technology or protection method. This should include the deployment of regularly updated firewalls as well as gateway antivirus, intrusion detection or protection systems (IPS), website vulnerability with malware protection, and web security gateway solutions throughout the network.
- Implement and enforce a security policy whereby any sensitive data is encrypted at rest and in transit. Ensure that customer data is encrypted as well. This can help mitigate the damage of potential data leaks from within an organization.
- Implement SMB egress traffic filtering on perimeter devices to prevent SMB traffic leaving your network onto the internet.
- Educate employees on the dangers posed by spear-phishing emails, including exercising caution around emails from unfamiliar sources and opening attachments that haven't been solicited. A full protection stack helps to defend against emailed threats, including Symantec Email Security.cloud, which can block email-borne threats, and Symantec Endpoint Protection, which can block malware on the endpoint. Symantec Messaging Gateway's Disarm technology can also protect computers from threats by removing malicious content from attached documents before they even reach the user.
- Understanding the tools, techniques, and procedures (TTP) of adversaries through services like DeepSight Adversary Intelligence fuels effective defense from advanced adversaries like Leafminer. Beyond technical understanding of the group, strategic intelligence that informs the motivation, capability, and likely next moves of the adversaries ensures more timely and effective decisions in proactively safeguarding your environment from these threats.

IOCs

Symantec has also developed a list of Indicators of Compromise to assist in identifying Leafminer activity:
