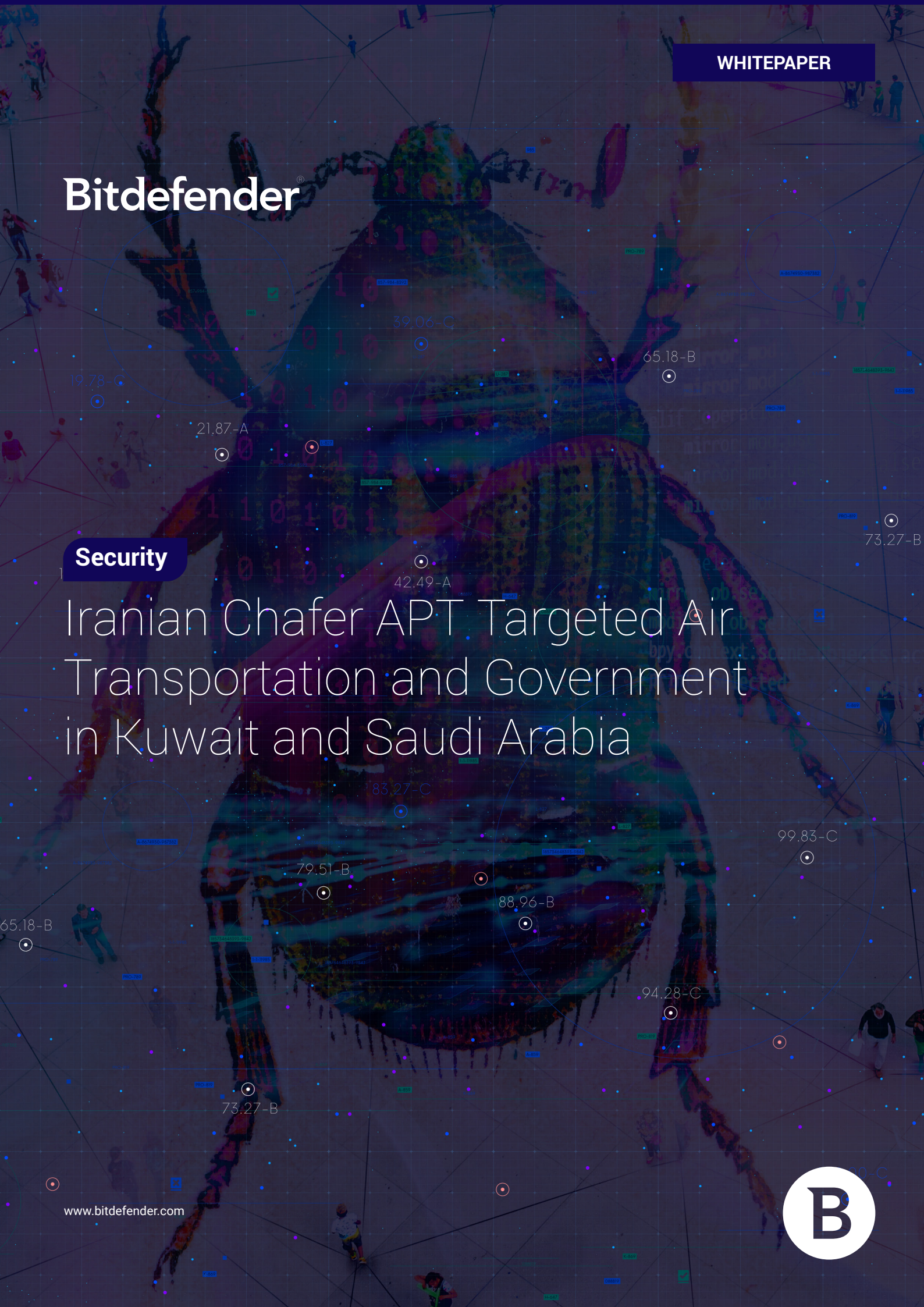
WHITEPAPER

Bitdefender



Security

Iranian Chafer APT Targeted Air Transportation and Government in Kuwait and Saudi Arabia

Contents

Author:

Bogdan Rusu Security Researcher

Overview

Chafer APT is a threat group with an apparent Iranian link. It is known to be active since 2014, focusing on cyber espionage campaigns. Bitdefender has spotted the group targeting critical infrastructure from the Middle East, presumably for intelligence gathering.

Bitdefender researchers have found attacks conducted by this actor in the Middle East region, dating back to 2018. The campaigns were based on several tools, including “living off the land” tools, which makes attribution difficult, as well as different hacking tools and a custom built backdoor.

Victims of the analyzed campaigns fit into the pattern preferred by this actor, such as air transport and government sectors in the Middle East.

Key Findings:

- Campaign targeted air transportation and government
- Attacker activity occurred on weekends
- In the Kuwait attack, threat actors created their own user account
- The Saudi Arabia attack relied on social engineering to compromise victims
- The end goal of both attacks was likely data exploration and exfiltration

Attack Lifecycle

Reviewing telemetry regarding this threat, we have identified victims from two countries, Kuwait and Saudi Arabia.

The modus operandi in these counties shares some common stages, but the attacks seem more focused and sophisticated on victims from Kuwait.

All the tools mentioned below will be detailed in the next section, *Tools Arsenal*.

Kuwait attack chain

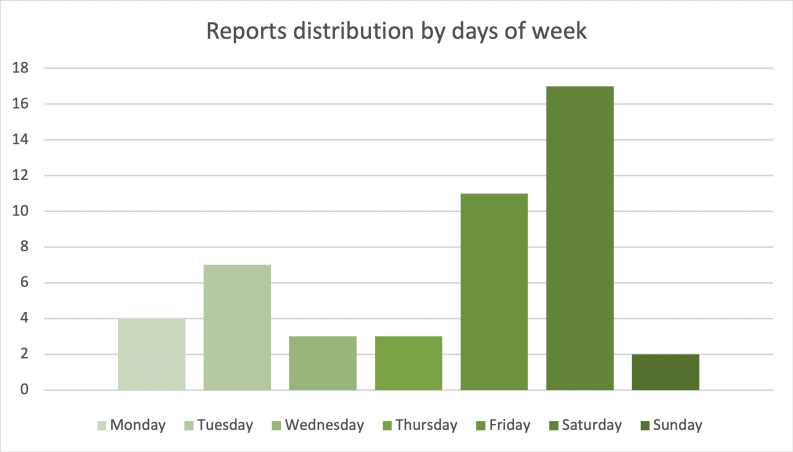
The first signs of compromise were several reverse TCP files and PowerShell commands that executed some base64 compressed code, specific to the Metasploit framework. Although difficult to speculate, it's possible that the threat actors used tainted documents with shellcodes to compromise the victim, potentially disseminated through spearphishing emails.

Once the victims were compromised, attackers started to bring reconnaissance tools for network scanning ("xnet.exe", "shareo.exe") and credential gathering (as "mnl.exe" or "mimi32.exe") or tools with multiple functionalities, such as CrackMapExec (for users' enumeration, share listing, credentials harvesting and so on). This arsenal of tools helped attackers move laterally inside the networks. Several methods were observed for this operation, either by using psexec for remote service installation (also used by one of their custom tools "step-1.exe"), or through the use of RDP protocol, a fact denoted by some unusual activity outside working hours and the presence of tools such as "rdpwinst.exe".

Once they gained a foothold inside the company, they started to install custom modules: a modified Plink (wehsvc.exe) installed as a service, as well as a backdoor (imjpuexa.exe), which was also executed as a service on some machines.

During our investigation, on some of the compromised stations we observed some unusual behavior performed under a certain user account, leading us to believe the attackers managed to create a user account on the victims' machine and performed several malicious actions inside the network, using that account.

- Some of the tools mentioned were found in an unusual place (on the Desktop), indicating that the account was not compromised.



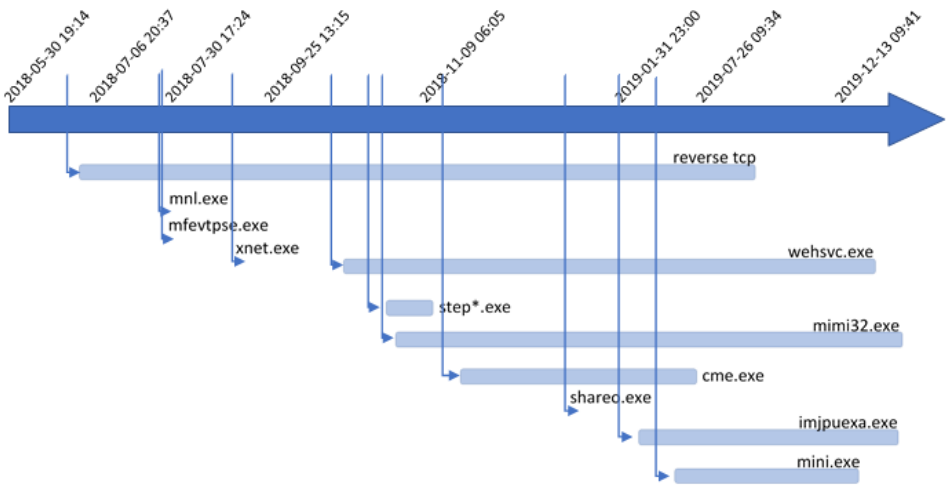
- Most activity occurs on Friday and Saturday, coinciding with the weekend in Middle East.
    - Reviewing the incident timeline, we observed the following sequence: deployment of the modified PuTTY tool ("*wehsvc.exe*") on one of the machines; a specific user is created four days after, on the same system; the user account is created on other systems from that network, during the following days;

- Beside the aforementioned tools, under this user account, we also saw the *rdpwinst* tool, which allows multiple rdp sessions management, Smartftp Password Decryptor - the installer, and Navicat Premium, a database management tool.

The attackers kept permanent communication with the victim, either through tools with proxy functionalities ("mfevtpse.exe" and "mini.exe") or through their own backdoor. As an interesting technique for C&C communication, we observed that the C&C address is actually passed as a command line argument (both for some of the proxy tools and for the backdoor itself).

Some traces indicate that the goal of the attack was data exploration and exfiltration (on some of the victim's tools such as *Navicat*, *Winscp,* found in an unusual location, namely "*%WINDOWS%\ime\en-us-ime*", or *SmartFtpPasswordDecryptor* were present on their systems). However, the lack of evidence, such as network logs, makes it difficult to confirm this was indeed the attacker's final objective.

A timeline of the attack for one of the organizations in Kuwait targeted by these threat actors is illustrated below.



Saudi Arabia attack chain

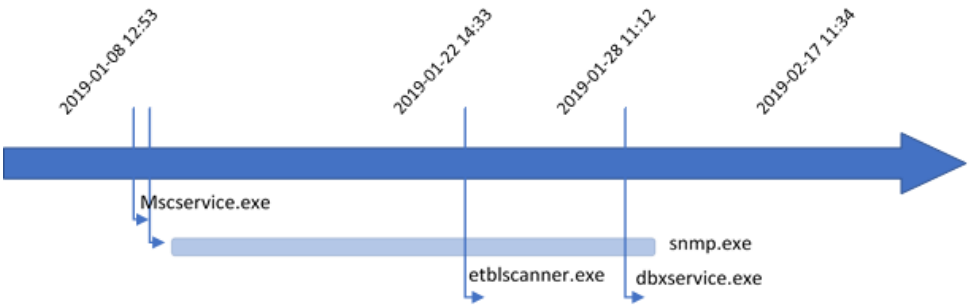
The case investigated in Saudi Arabia was not as elaborate, either because the attackers did not manage to further exploit the victim, or because the reconnaissance revealed no information of interest.

We suspect the initial compromise was achieved through social engineering. The RAT component was located in the *%Download%* folder, which is the default folder for any download process, while its parent process was actually *explorer.exe;* indicating that the user executed the malicious file. Also, the RAT was executed twice, with different names ("drivers.exe" and "drivers_x64.exe"). The two executions were three minutes apart, which raises suspicion that the user was tricked into running them.

Internal network reconnaissance seems to have been performed using the "etblscanner.exe" tool. We also spotted the use of three different RAT components which, according to the timeline, are not used at the same time. One of those components, "*snmp.exe*", is also present on some of the victims in Kuwait, under the name "*imjpuexa.exe*", linking these attacks to the same threat actors.

While this attack was not as extensive as the one in Kuwait, some forensic evidence suggests that the same attackers might have orchestrated it. Despite the evidence for network discovery, we were not able to find any traces for lateral movement, most probably because threat actors were not able to find any vulnerable machines.

A timeline of the attack is illustrated below.



Tools arsenal

Living off the land tools

This threat actor heavily uses "the Non-Sucking Service Manager" for ensuring that its critical components, such as the proxy or the *RAT,* are up and running. They also use Sysinternals tools, such as psexec, for lateral movement in the victim's network. In terms of preinstalled Windows tools, we spotted the use of "schtasks.exe" for ensuring persistence, "*tasklist*" for testing persistence, and "*nslookup*" for communication over DNS, making queries for *TXT* record.

Hacking tools

By analyzing reports from targeted victims, we also spotted hacking tools usually used in different stages of the kill chain.

Mimikatz was used with different flavors, such as SafetyKatz, or customized, as depicted by previous security researchers. The credentials obtained were used with the *psexec* tool to gain access to specific machines, a fact denoted by some Python scripts converted to executables, which make the appropriate call to *psexec* with plain text credentials.

Some infected systems also contain pieces of shellcode from the Metasploit framework, such as *reverse_tcp*, with the purpose of connecting to different internal IP addresses.

Another tool, the CrackMapExec executable for version 2.2 (found on GitHub), has functionalities such as network scanning and credential dumping, as well as accounts discovery or code injection.

Custom build tools

PLINK Tool

A slightly modified version of PLINK, part of the PuTTY suite, was also revealed by Bitdefender telemetry in late September 2018. It preserves the original functionality, with some key new features such as the possibility to run it as a Windows service or to uninstall the service. We believe this tool may have been used either to communicate with the CnC or to gain access to some internals machines, but found no conclusive evidence to support these scenarios. As filenames, we've seen only one name: "*wehsvc.exe*".

Proxy Tools

Beside PLINK, we spotted a command line tool, written in C++, that implements a proxy. The architecture of this application is straightforward, imposing the following flow:

- it connects to the first available server from a given list
- sends the following HTTP header `"GET /CNT HTTP/1.1\r\nHost: bing.com\r\nUser-Agent: Mozilla/5.0"`, to indicate the beginning of the communication
- waits for the server for a limited time, which will send a byte, representing a command and the associated message.

The exposed commands are for setting or viewing the proxy id, echoing, session resetting, starting a tunnel or exiting.

Tunneling option (also denoted by debugging strings), which is the main functionality of this component, implements socks5 protocol. When this command is selected, the proxy starts a new *tcp* connection with the current server, sending the following http header *"*`GET /TNL HTTP/1.1\r\nHost: bing.com\r\nUser-Agent: Mozilla/5.0"`. Then, it switches to the socks5 protocol on a new thread.

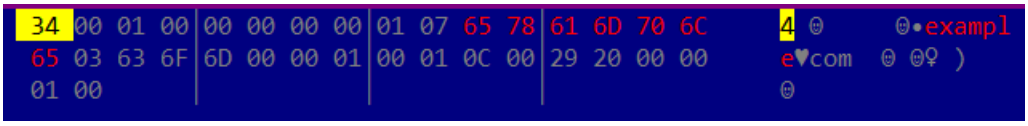
On some systems where we found this file, we noticed another proxy, different from the previous one. In terms of implementation, it uses a custom protocol, which implies using a table of available connections and their ids. Those ids are used in sending messages between hosts. Also, this one was packet by the *UPX packer*, version 3.03.The main purpose of this tool is to give the attacker access to the internal network of the victim.

In our telemetry, those files were seen with the name of "*mini.exe*", "*mfevtpse.exe*" or "*mfevtps.exe*".

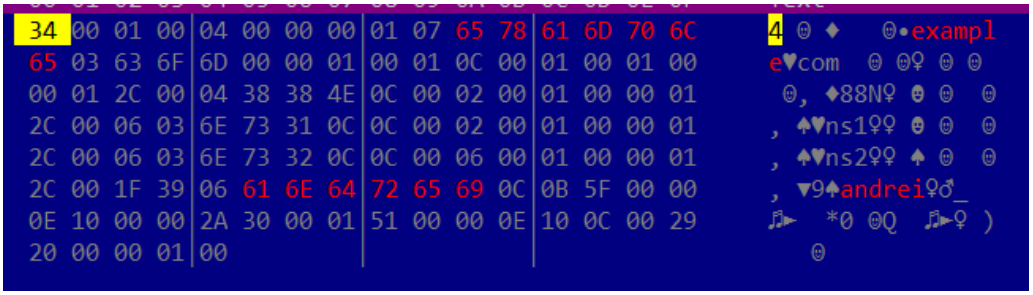
RAT Tools

During the attack, we also observed the use of a command line utility, which is a RAT, written in Python (probably version 3.4) and converted into a standalone executable. Interestingly, the user interacts with this tool in a similar way as with "mini.exe", described in the *Proxy Tools* section. The same filename for default input, the common debugging strings, even the help page for the two are very similar, which suggests a possible connection between the two.

This tool uses 2 types of communications ("D*NS"* and *"HTTP"*, as found in code), both over TCP, with the same functionality. They both marshal the message such that the packet will resemble a *DNS*, and *HTTP*, packet. Parts of the headers that are hardcoded can be seen below.



Part of header that will be included in the request (dns communication)



Part of header that will be included in the response (dns communication).

Headers for http communications are "*GET /owa HTTP/1.1\r\nHost: live.com*" for request and "*HTTP/1.1 200 OK*" for response. Also, some parts of the code are specific to different operating systems, which means that this tool may be in the wild in other forms.

Filenames for these tools found in our telemetry are "*snmp.exe*", "*imjpuexa.exe*" and "*driver_x86.exe*".

Our telemetry for the same machines revealed two other files that implement RAT functionalities, besides "snmp.exe"and"imjpuexa.exe".

One of them is very similar to *MechaFlounder*, as described by previous security research, but packing a few new features. It implements a persistence mechanism (using a scheduled task, named "*Defender Update*") and a custom communication protocol over *DNS (*besides *HTTP)* with the CnC, where the response is found either in the IPv4 address or in the *TXT* record.

The second file is also about persistence and features a similar mechanism for parsing commands as the previous file. However, it uses the *"Service Update"* scheduled task name, instead of *"Defender Update".* The key difference between the two files is that the latter, in this case, communicates with the CnC through files uploaded to Dropbox, where each victim has a separate folder named with the same combination of username and machine name as used by *MechaFlounder*. The command, "service.html" is placed in the root of this directory, uploaded files from the victim

are placed into a folder named "/download", and the files for download are placed into the "/upload" folder. Also, all feedback messages are simplified and uploaded in the same directory, under the name "results.txt". It also implements a synchronization mechanism by using the folder "done", placed in the root location for each victim.

Filenames for the two RATs are: "*drivers.exe*" ("*drivers_x64.exe*" for the 64-bit version) and "*dbxservice.exe*". In terms of persistence, both "*drivers_x64.exe*" and "*dbxservice.exe*" make a copy of themselves in the *Temp* folder, named "*MSCService.exe*", or "*DBXService.exe*" and then create a scheduled task that will reference them in that location. Another interesting thing found in the decompiled code of the two files is the use of the special Unicode character "202e" (Right-to-Left Override character), in the persistence section. This character is expected to be found as the first command line argument.

Scanning tools

Bitdefender telemetry revealed another command line tool used in this attack, "*xnet.exe*", which is very similar to the known *nbtscan tool*, except it packs an additional feature. This version of the tool also obtains the IP range to scan (when there is no given range) from network adapters on the machine. We also observed another tool, ("shareo.exe") written in C#, which obtains the NetBIOS name for each machine within a range of IPs.

Further investigation into our telemetry revealed a new tool ("*etblscanner.exe*"), implemented in Python and converted to a Windows executable. As the name implies, it's an EternalBblue scanner that accepts a given range of IPs.

Remexi tool

Found as "*mas.dll*" in our telemetry, it has been previously depicted as a backdoor. Interestingly, there is a connection between this file and the "*xnet.exe*" tool described in the *Scanning tools* section above, as indicated by some very similar yet uncommon *pdb* paths:

- "*F:\Projects\94-06\RCE\bin\Release\x64\mas.pdb*" – in "mas.dll" tool
- "*F:\Projects\94-08\XNet\bin\Release\Win32\XNet.pdb*") – in "xnet.exe" tool

These two tools also share common functions in their code, some of them for debugging purposes. Both have the same build number, 51106, for the compiler and the linker, which is found in the Rich header, and, in the PE header they have the same Major.Minor version, namely 11.0. Thus, these metadata suggest an even stronger relationship between them.

MITRE matrix TTPs

https://attack.mitre.org/groups/G0087/

Tactic: Persistence

Technique: T1050 "New Service":

"wehsvc.exe" hasthe ability to create a service and *"imjpuexa.exe"* was spotted in the registry "*HKLM\system\controlset001\services\microsoft updating\parameters\application"*

Technique: T1053 "Scheduled Task":

Both"*MSCService.exe*" and "*DBXService.exe*" use this technique

Technique: T1136 "Create Account":

Suspicious reports from a user's desktop folder, including similar behavior from some of the aforementioned tools

Tactic: Discovery

Technique: T1016 "System Network Configuration Discovery":

The "*xnet.exe*" component implements *nbtstat* functionality for a range of addresses

Tactic: Command and Control

Technique: T1090 "Connection Proxy":

Tools in the *Proxy Tools* section are candidates for this technique.

Tactic: Defense Evasion

Technique: T1045 "Software packing":

The "*mfevtpse.exe*" component uses this kind of technique, leveraging the UPX packer.

Technique: T1036 "Masquerading":

Both "DBXService.exe" and "MSCService.exe" include instances where their name contains the special RLO character "\u202e". The "*%WINDOWS%\ime*" and "*%LOCALAPPDATA%\micrososft\taskbar*" folders are used for deploying tools using the same technique

Tactic: Execution

Technique: T1059 “Command line interface”:

Most of the enumerated tools use a command line interface

Tactic: Credential Access

Technique: T1003 “Credential Dumping”:

The use of Mimikatz on affected systems for credential dumping

Appendix

IoC type	IoC value	Alias
sha256	5ee9873c3c8684ac097bd28d3caf4264c6da6aa6acfeb8f6e72f1a99215a4be8	*xnet.exe*
sha256	710e32af0d41a6701d57337701b091b158add04a601b68cca67a808bdd87d881	*snmp.exe* *imjpuexa.exe* *driver_x86.exe*
sha256	d965352c6632e694b8f1f62f96874bd0df8d7c128c465ee9a76eb86ebddb0c02	*drivers.exe* *drivers_x64.exe*
sha256	11dbfb390f7008524e523da7d0cda61723584082fc91ff96d1148c4aac6198a0	*dbxservice.exe*
sha256	c839e886b98d2c752a134e888dad40799cd9966f8a73b51edc85ca2d72f99616	*mfevtpse.exe*
sha256	144a160c57c2d429d072046edfdd1b44ff22bcae4f0535732f6c2b19190f2f35	*wehsvc.exe*
sha256	508ba7971b1f7651ba7d26815f75d66977820bd4eb3a615e3ab7079058d80380	*mimi32.exe*
sha256	f991cadf11c5075f0ed6f381dfdac311cf59480962debf8b874f95e9bee5c4f2	*mnl.exe*
sha256	021813c78cf31b0d7e77b40374347d8ed4e5a5ca69a7fc29bbc7bff969c09f3c	*shareo.exe*
sha256	b297a0b2e775f096d9ebda6130abbb5ec59813c7703159ea191b47d7b7293e1e	*etblscanner.exe*
sha256	a1f5c72721f9aa2ca29f1de7645a64b505c05dcd53dbdd7b9e904b1627c6d578	*mini.exe*
sha256	98a9b2329eefe618daa78b6afed82cebf40cb918ad0aae7a8d7f59af4cb13b41	*mas.dll*
domain	dropboxengine[.]com	
domain	redjewelry[.]biz	
domain	apigoogle-accounts[.]biz	
domain	update-microsoft[.]space	

Proudly Serving Our Customers

Bitdefender provides solutions and services for small business and medium enterprises, service providers and technology integrators. We take pride in the trust that enterprises such as **Mentor, Honeywell, Yamaha, Speedway, Esurance or Safe Systems** place in us.

Leader in Forrester's inaugural Wave™ for Cloud Workload Security

NSS Labs "Recommended" Rating in the NSS Labs AEP Group Test

SC Media Industry Innovator Award for Hypervisor Introspection, 2nd Year in a Row

Gartner® Representative Vendor of Cloud-Workload Protection Platforms

Dedicated To Our +20.000 Worldwide Partners

A channel-exclusive vendor, Bitdefender is proud to share success with tens of thousands of resellers and distributors worldwide.

CRN 5-Star Partner, 4th Year in a Row. Recognized on CRN's Security 100 List. CRN Cloud Partner, 2nd year in a Row

More MSP-integrated solutions than any other security vendor

3 Bitdefender Partner Programs - to enable all our partners – resellers, service providers and hybrid partners – to focus on selling Bitdefender solutions that match their own specializations

Trusted Security Authority

Bitdefender is a proud technology alliance partner to major virtualization vendors, directly contributing to the development of secure ecosystems with **VMware, Nutanix, Citrix, Linux Foundation, Microsoft, AWS, and Pivotal.**

Through its leading forensics team, Bitdefender is also actively engaged in countering international cybercrime together with major law enforcement agencies such as FBI and Europol, in initiatives such as NoMoreRansom and TechAccord, as well as the takedown of black markets such as Hansa. Starting in 2019, Bitdefender is also a proudly appointed CVE Numbering Authority in MITRE Partnership.

RECOGNIZED BY LEADING ANALYSTS AND INDEPENDENT TESTING ORGANIZATIONS

CRN AV-TEST AV Gartner 451 Research FORRESTER IDC GLOBAL

TECHNOLOGY ALLIANCES

Microsoft NUTANIX aws Pivotal Cloud Foundry CITRIX

Bitdefender

Founded 2001, Romania
Number of employees 1800+

Headquarters
Enterprise HQ – Santa Clara, CA, United States
Technology HQ – Bucharest, Romania

WORLDWIDE OFFICES
USA & Canada: Ft. Lauderdale, FL | Santa Clara, CA | San Antonio, TX | Toronto, CA
Europe: Copenhagen, DENMARK | Paris, FRANCE | München, GERMANY | Milan, ITALY | Bucharest, Iasi, Cluj, Timisoara, ROMANIA | Barcelona, SPAIN | Dubai, UAE | London, UK | Hague, NETHERLANDS
Australia: Sydney, Melbourne

UNDER THE SIGN OF THE WOLF

A trade of brilliance, data security is an industry where only the clearest view, sharpest mind and deepest insight can win — a game with zero margin of error. Our job is to win every single time, one thousand times out of one thousand, and one million times out of one million.

And we do. We outsmart the industry not only by having the clearest view, the sharpest mind and the deepest insight, but by staying one step ahead of everybody else, be they black hats or fellow security experts. The brilliance of our collective mind is like a **luminous Dragon-Wolf** on your side, powered by engineered intuition, created to guard against all dangers hidden in the arcane intricacies of the digital realm.

This brilliance is our superpower and we put it at the core of all our game-changing products and solutions.

Bitdefender-PR-Whitepaper-Chalet-cresta4451-en_EN
05/07/20May 15 2020 10:14 am05/15/20