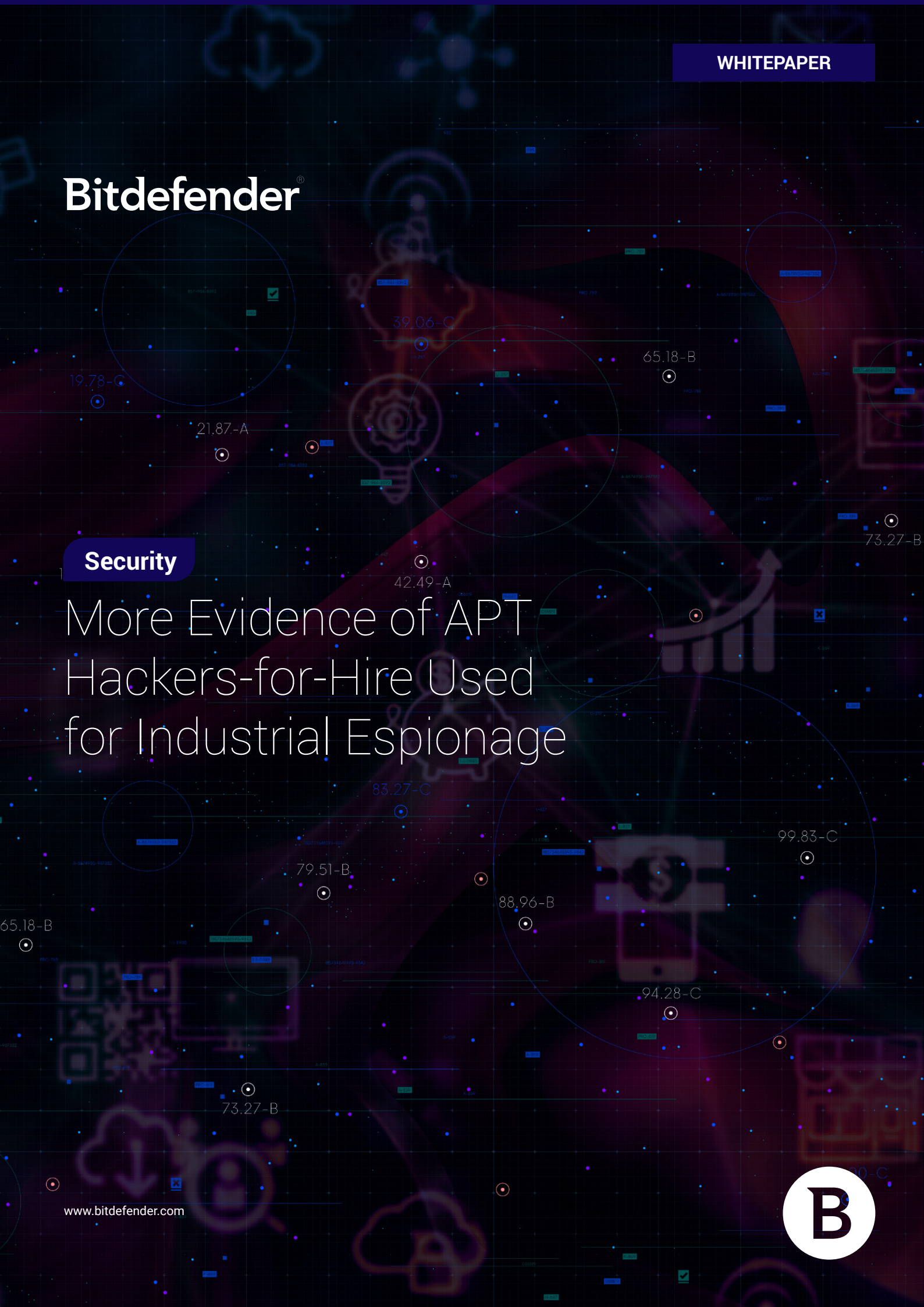
WHITEPAPER

Bitdefender



Security

More Evidence of APT Hackers-for-Hire Used for Industrial Espionage

www.bitdefender.com

Contents

Authors:

Victor Vrabie- Security Researcher, Cyber Threat Intelligence Lab

Bogdan Rusu - Security Researcher, Cyber Threat Intelligence Lab

Alexandru Maximciuc -Team Lead, Cyber Threat Intelligence Lab

Co-author:

Cristina Vatamanu - Senior Team Lead, Cyber Threat Intelligence Lab

Executive Summary:

Bitdefender researchers recently investigated a sophisticated APT-style cyberespionage attack targeting an international architectural and video production company, pointing to an advanced threat actor and a South Korean-based C&C infrastructure.

As per reports in the past, APT mercenary groups have been used for cyberespionage by private competing companies seeking financial information or negotiation details for high-profile contracts. This attack likely falls under the same category. APT mercenary groups have been known to offer their services to the highest bidder, deploying sophisticated attacks and powerful cyberespionage tools against their contracted victims. The StrongPity APT group is one such example that Bitdefender investigated recently. The group, which has been known to target select victims, was recently associated with a potential Turkish military operation.

The commoditization of APT-level hackers-for-hire could potentially entice rival luxury real-estate investors involved in multi-billion-dollar contracts to seek these services to spy on their competition by infiltrating their contractors. Industrial espionage is nothing new and, since the real-estate industry is highly competitive, with contracts valued at billions of dollars, the stakes are high for winning contracts for luxury projects and could justify turning to mercenary APT groups for gaining a negotiation advantage.

The targeted company is engaged in architectural projects with billion-dollar luxury real-estate developers in New York, London, Australia and Oman. With offices in London, New York, and Australia, the company's customers and projects involve luxury residences, high-profile architects and world-renowned A-list interior designers.

The sophistication of the attack reveals an APT-style group that had prior knowledge of the company's security systems and used software applications, carefully planning their attack to infiltrate the company and exfiltrate data undetected.

The Bitdefender investigation revealed the cybercriminal group infiltrated the company using a tainted and specially crafted plugin for Autodesk 3ds Max (popular software widely used in 3D computer graphics). The investigation also found that the Command and Control infrastructure used by the cybercriminal group to test their malicious payload against the organization's security solution, is located in South Korea.

During the investigation, Bitdefender researchers also found that threat actors had an entire toolset featuring powerful spying capabilities. Based on Bitdefender's telemetry, we also found other similar malware samples communicating with the same command and control server, dating back to just under a month ago. Located in South Korea, United States, Japan, and South Africa, it's likely the cybercriminal group might have also been targeting select victims in these regions as well.

Key Findings:

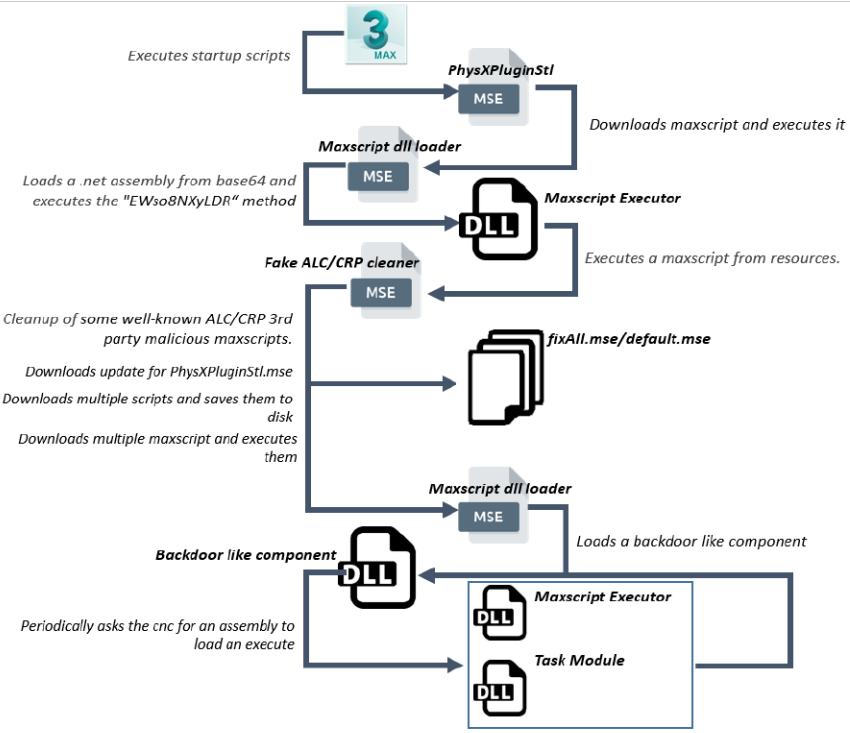
- Potential APT mercenary group used for industrial cyberespionage
- Industrial espionage for competitiveness in real-estate industry
- Malicious payload posing as a plugin for a popular 3D computer graphics software (Autodesk 3ds Max)
- Payload tested against the company's security solution to avoid detection upon delivery
- C2 infrastructure based in South Korea

While this is not the first incident in which APT mercenary groups have been potentially used to conduct espionage or coordinate with alleged military operations, these events have intensified during the past couple of years. The recently investigated StrongPity APT group has all the characteristics of a mercenary cybercriminal group, known to serve both financial and potentially military objectives. Other groups, such as "Dark Basin" and "Deceptikons," are only a few recent examples in which APT groups for hire have allegedly acted on behalf of customers seeking to discredit or infiltrate high-profile targets in financial, legal, and now the multi-billion-dollar real-estate industry.

This is likely to become the new normal in terms of the commoditization of APT groups -- not just state-sponsored actors, but by anyone seeking their services for personal gain, across all industries.

Forensic Analysis

The threat forensic analysis started from a suspicious sample named `PhysXPluginStl.mse` (hash: `d6ad1e0b11a620ed4df39255ffff11a483687d7038d6c76b938d15add54345fa`) which triggered suspicious behavior.



Attack overview

In a recent advisory published by Autodesk, users are warned of a third-party MAXScript exploit, “PhysXPluginMfx” (variant of ALC2, ALC, CRP and ADLS), that can corrupt 3ds Max to run malicious code and even propagate to other MAX files. Instructions on how to identify and remove the malware have also been published. However, as our investigation revealed, it’s likely that more victims were affected long before this unknown threat was identified.

The file is a Max Script Encrypted script (encryption specific to Autodesk 3dsMax Solution software) and contains an embedded DLL file (hash: `2d934a705638acd3fcb44f66a9a1633c27231550113f20df6061c10b1aa6e9f6`). Further analysis of this file lead us to a maxscript that starts with some http post requests, whose responses are executed directly from memory, after some delays. Those two requests are the following:

- POST, hxxp://175[.]197.40.61:3445/FRNuzqJIZyb, using a token in body: “t785EyDk/6s4VXZZ6Sb7TFl7vepBKQrgX8LmGURaPLM=”, without any additional information; the execution is postponed 10 seconds
- POST, hxxp://175[.]197.40.61:3445/TYEHVSjn2Ny, using a token in body: “RhUzq3wdz8xpCIzZVoqrTDr0FXpOmsgjAnyTy6xh/+w=”, without any additional information; the execution is postponed 4 seconds

Moving further, a periodic job is created to clean up some well-known ALC/CRP 3rd party maxscripts, which are known to lead to some issues (see the `Appendix A` for more information about these issues). This part may look unsuspicious, but, after cleanup, some code is downloaded from the C&C and executed. The download is performed from the following URLs:

- hxxp://175[.]197.40.61:3445/Public/Find_Alc
- hxxp://175[.]197.40.61:3445//Public/Find_Crp

The last part of the script takes care of the persistence. A downloaded file (from `hxxp://175[.]197.40.61:3445/grhL1wCYAhf`) is stored in "`AppData\Local\Autodesk\3dsMax\*\ENU\scripts\startup\PhysXPluginStl.mse`" (in the startup folder of 3ds max software) and the hidden file attribute is set.

Investigating the C&C, we managed to reproduce part of the communication protocol and to download buffers of code whose content is executed. Responses from the C&C were valid, indicating that, at the time of the writing, it was still up. The response for the route `hxxp://175[.]197.40.61:3445/FRNuzqJIZyb`, lead us to two new files (`a32f5e65051eb95d0ccdcc899d45f56369659a6edea068da5e59951f4c903f7b` and `c75fcb34a5b35b6b73191de3f342806d3cce5a446c64f55fb3423f0cd5dbe248`), which are .net binaries. Both of them will download and execute other maxscripts whose content is very similar.

The new script is meant to collect some information about the victim (computer name, username), encrypt it with a custom algorithm and mask the result so that it appears to be base64 content. Moving further, the obtained data is used in a request sent to the C&C (at `hxxp://175[.]197.40.61:3445/TYEHVSjn2Ny`), to obtain a new piece of code to be executed. After this, for each 3ds max release, installed on the machine, in `scripts\startup\max` folder a file named "`default.mse`" is downloaded from `hxxp://175[.]197.40.61:3445/YkSxBJVz` using the aforementioned user information, and then, detection evasion techniques are applied (file creation timestamp is modified, the hidden attribute is set on the max folder and the `default.mse` file. In this case also, a cleanup action is performed, similar to the one mentioned above, which cleans up some well-known ALC/CRP third-party maxscripts.

The response for the `hxxp://175[.]197.40.61:3445/TYEHVSjn2Ny` request, leads us to a .net assembly (`04715dd5b4e4e4e452d86f2c874ea9e6ad916f17838f116c8ab4ccfc7b9b6657`) whose resource section contains a downloader, which obtains from the C&C (`hxxp://175[.]197.40.61:3445/b route`), other binaries. We were unable to obtain the responses directly from the C&C, but, based on some quite unique method names invoked by the downloader we managed to obtain a binary (`1c2f754045bc442cf5147dadccd1ff3c8e58205362e1940c3f1f87ab303006a5`). This malicious file is capable of making screenshots, collecting passwords and history from a Chrome browser database. This information is uploaded to the C&C, the same as in our case, strengthening the idea of being the one requested by the downloader.

It is not uncommon in targeted attacks for the threat actors to test malicious files against the security solutions used by their victims, so that they can change them until the files are no longer detected.

We have also identified a toolset that is described in section below. We have chosen a representative file for each category, all the indicators of compromise being listed in the `Appendix B` section.

Toolset Analysis

Looking through the telemetry of the C&C, we noticed that there are reports, which include some of the discovered .net assembly internal names found initially on the victims' machine or downloaded from the C&C. After analysis, we have managed to gather more tools, based on direct usage or based on common portions of code. Beside this, we have also noticed that all of them share the C&C address from the victim (address + port).

HdCrawler

Representative binary: `a16b2c6a60975e4def1f799c69f7f38064653b5a99bc577fc008f0a808c7bc62`

The binary's role is to list, compress (if needed) and upload a list of specific files (searched by extension). Caution has been taken not to apply useless compression – if the file to be copied has the extension in this list:

`".zip", ".rar", ".alz", ".7z", ".mp4", ".flv", ".webm", ".webp", ".jpg", ".jpeg", ".png", ".avi", ".mkv", ".mp3", ".mpeg", ".mpg", ".apk", ".obb", ".pur", ".uasset"`

then the file is skipped from compression.

There is an interesting aspect to this component – the list of files to be uploaded to the server is built into the binary, which means that, on the other side, the attackers look at the file listings from each of their victims and then compile a HdCrawler binary specific to the victim.

While searching for more related samples and information, we found two "tools" that should be on the C&C side, used to control and manage the victims and the stolen information by processing the output of the HDCrawler:

- LogViewer – a tool with a GUI that seems to be the one that shows the victims and the file listings from them
- HddUnpacker - is used by LogViewer to decrypt and decompress the files uploaded by HdCrawler, the screenshots taken during the attack, the file listings, and the credentials stored in the Chrome browser

InfoStealer

Representative binary: `2b394c330949c85097f13eded38f08b358d399b7615bbe3659dd9d82ec82675c`

`PhysXPluginStl.mse`, `2d934a705638acd3fcb44f66a9a1633c27231550113f20df6061c10b1aa6e9f6` file mentioned before has the OriginalFilename set to `B4E6HVVnCvY.dll`. In our file repositories we have found a file (`2b394c330949c85097f13eded38f08b358d399b7615bbe3659dd9d82ec82675c`) with OriginalFilename set to `B4E6HVVnCvY.exe`. There is high confidence that this sample is related, also because of the use of the same C&C.

This binary has the following capabilities:

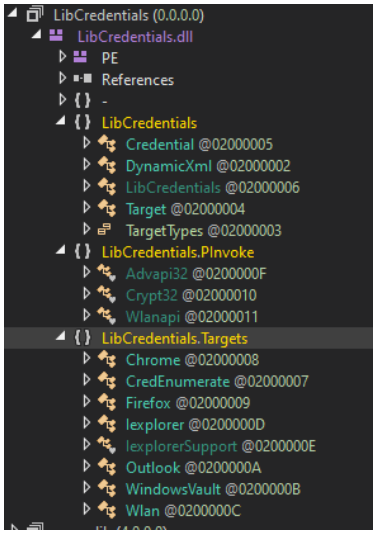
- **Rate-limiting** - uses `%LOCALAPPDATA%\ Microsoft\Internet Explorer\MSWINSIG.DAT` (in which it writes a timestamp) as a rate-limiting mechanism, to run at most once every three hours
- **Screen capture** – makes whole screen capture and uploads it to the C&C server
- **Information collection** – collects the username, computername, the IP addresses of network adapters, Windows ProductName, version of the .NET Framework, information about the processors (number of cores, the speed and other information), total and free RAM, information about the storage, the listing of files set to start automatically when Windows starts up, process listing and recent files; all this information is uploaded to the C&C server.
- **Tied to a specific user on the computer** - uses `%LOCALAPPDATA%\ Microsoft\Internet Explorer\ MSWINTAP.DAT` – the first four bytes of it contain a hash on the computername and username; that hash is checked before the content gets loaded; the remaining bytes are received from the C&C and are appended to the following http request messages to the C&C;
- It makes use of another file "tied" to the user (same hash as in the case of `MSWINTAP.DAT`) in %PROGRAMDATA%\ Microsoft\Windows\Ringtones; we know it writes 11 characters in it, but its exact intention is yet to be discovered
- `%LOCALAPPDATA%\ Microsoft\Internet Explorer\ie4uRidd.dat` – it's a .NET class (named internally TaskClass), serialized and encrypted, which represents a task for file listings; it contains a list of disk drives and specific directories that will be recursively listed from now on. This mechanism lets the attackers skip specific directories and disk drives completely and get back only information about the files they are most interested in. If this `ie4uRidd.dat` file is not present, then a directory listing of all files from B:, C:, D:, K: is sent to the C&C server (we couldn't find out why these specific drives were chosen).

Observations

The authors took an interesting approach to avoid attracting attention. If Task Manager or Performance Monitor applications are running and their respective window is visible, then a flag is set, depending on how much of the area is visible to the user; this flag instructs the binary to sleep more and more often (reducing this way the consumption of CPU).

An interesting library we could link to this whole toolkit is `LibCredentials`.

We did not see it used anywhere in our telemetry. According to the class names, it's responsible for collecting credentials from the current machine: browsers (Internet Explorer, Firefox, Chrome), Outlook, WLan credentials and everything stored in Windows Vault.



Command and Control Server

The C&C belongs to AS4766 Korea Telekom, South Korea. Although Shodan (`hxxps://beta.shodan.io/host/175.197.40.61`) suggests that there are many different ports on the C&C server (and most of those ports can be seen on other IPs too), we have only seen components that communicate to port 3445 and port 6711. (the latter is used by a FTP server, as can be seen in the HdCrawler binaries we found).

Appendix A

Details about ALC/CRP 3rd party maxscripts:

https://3dground.net/article/attention-alc-and-crp-viruses-in-3ds-max-

Appendix B – IOCs

File Hashes:

- 04715dd5b4e4e4e452d86f2c874ea9e6ad916f17838f116c8ab4ccfc7b9b6657
- 1c2f754045bc442cf5147dadccd1ff3c8e58205362e1940c3f1f87ab303006a5
- A32f5e65051eb95d0ccdcc899d45f56369659a6edea068da5e59951f4c903f7b
- C75fcb34a5b35b6b73191de3f342806d3cce5a446c64f55fb3423f0cd5dbe248
- 2d934a705638acd3fcb44f66a9a1633c27231550113f20df6061c10b1aa6e9f6
- d6ad1e0b11a620ed4df39255ffff11a483687d7038d6c76b938d15add54345fa
  2b394c330949c85097f13eded38f08b358d399b7615bbe3659dd9d82ec82675c
- A16b2c6a60975e4def1f799c69f7f38064653b5a99bc577fc008f0a808c7bc62
- E16a5847ac62bb4d5a661863fd5dba5201d27784e280aeee25a34702ed4c1528
- C2f51b2c116bcc9c95dbf567a90ec4fe0f5fbddb066a6d3cdf814295838e00f8
- D3a38047c207dee4b09d607a568390306f76025cd6986ec3e7c3fbd21a231d0e
- 37ea55d1dceb467c595299f0f19a68d5530015b6d9c7ed5cc16324f52773e536
- 711d45ff150aa734771fec1c08e394118a7bcd015dacac8889c965aeabfc7c9d
- 07cebf1d377b9d28e53b7139a56e632e19c8f53e07546298f180322d462512e3
- 536ef8065ded253465d6a5a967dafdcb2d158a7ea3157f0b265788745ed38409
- 9e4ba32d42f26b7b3bb24ec786992ed017318a4074b2e141ad0f4a05435f4862

File Names:

- PhysXPluginStl.mse
- fixAll.mse
- default.mse
- %LOCALAPPDATA%\ Microsoft\Internet Explorer\MSWINTAP.DAT
- %LOCALAPPDATA%\ Microsoft\Internet Explorer\MSWINSIG.DAT
- %LOCALAPPDATA%\ Microsoft\Internet Explorer\ie4uRidd.dat

URLs:

- hxxp://175.197.40[.]61:3445/eYOMAHg
- hxxp://175.197.40[.]61:3445/YkSxBJVz
- hxxp://175.197.40[.]61:3445/n
- hxxp://175.197.40[.]61:3445/r
- hxxp://175.197.40[.]61:3445/l
- hxxp://175.197.40[.]61:3445/b
- hxxp://175.197.40[.]61:3445/TYEHVSjn2Ny
- hxxp://175.197.40[.]61:3445/grhL1wCYAhf
- hxxp://175.197.40[.]61:3445/Public/Find_Alc
- hxxp://175.197.40[.]61:3445//Public/Find_Crp
- hxxp://175.197.40[.]61:3445/FRNuzqJIZyb
- hxxp://175.197.40[.]61:3445/Public/fixAll
- hxxp://175.197.40[.]61:3445/Public/NlWuLNUDzqM

C&C IP addresses:

- 175[.]197[.]40[.]61

Why Bitdefender

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-APT-Hackers-creat-ref7470-en_EN
08/19/20August 19, 2020 3:04 pm08/19/20