

"Light, Dark and... a Sunburst: Dissection of a very sophisticated attack"

Who we are: Stefano

- I am a Senior Principal Consultant for Incident Response and a leading figure of the RSA IR Team.
- I begun my ICT career in 1997 in Digital Corp, but I started to crack software in 1985 with a Commodore C64...
- I decided to get out of the cracking scene in 2000 and for about three years I remained focused on Networking and System administration... until Nimda and Blaster came out and testing network and system security became an interesting career...
- I worked on the testing and offensive side until 2009 when I jumped into the IR bandwagon.
- Since then I got busy with engagement around the world... covering investigation in banks, military, governments and telco companies.



Who we are: Alessandro

- Today: EMEA Incident Response Consultant @ RSA
- Past: 22 years of experience
- Love hunting and intelligence
- A proud dad and happy husband

Sunburst: the story, the tools, the IOCs

In the beginning it was Fireeye...

Our story begins on December 8th 2020, when Fireeye publicly states on a post in her website that she was targeted by a sophisticated actor.



Home > FireEye Blogs > FireEye Stories > FireEye Shares Details of Recent Cyber Attack, Act...

FireEye Stories

FireEye Shares Details of Recent Cyber Attack, Actions to Protect Community

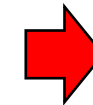
December 08, 2020 | by Kevin Mandia

FIREEYE TOOLS RED TEAM

FireEye is on the front lines defending companies and critical infrastructure globally from cyber threats. We witness the growing threat firsthand, and we know that cyber threats are always evolving. Recently, we were attacked by a highly sophisticated threat actor, one whose discipline, operational security, and techniques lead us to believe it was a state-sponsored attack. Our number one priority is working to strengthen the security of our customers and the broader community. We hope that by sharing the details of our investigation, the entire community will be better equipped to fight and defeat cyber attacks.

In addition, the attacker stole specific tools:

During our investigation to date, we have found that the attacker targeted and accessed certain Red Team assessment tools that we use to test our customers' security. These tools mimic the behavior of many cyber threat actors and enable FireEye to provide essential diagnostic security services to our customers.



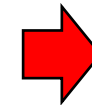
The attacker focused on specific Customers data, in particular that the Governmental Agencies:

Consistent with a nation-state cyber-espionage effort, the attacker primarily sought information related to certain government customers.



Since the beginning the hypothesis was about a «State-sponsored Attacker»

...



In the beginning it was Fireeye...

Fireeye promptly gave IOCs to identify and track the attacker, his malicious tools and the attacker TTPs in a Github:


fireeye / red_team_tool_countermeasures

<> Code ⓘ Issues 1 🔗 Pull requests 2 🛡 Security 📄 Insights

🔗 master ▾ 🌿 1 branch 🏷 0 tags

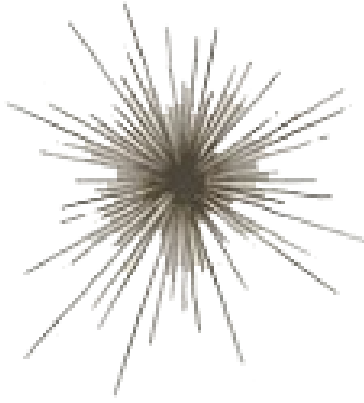
Go to file

↓ Code ▾

 mikesiko	Update signatures_table_of_content.csv	1b90ba7	19 days ago	🕒 36 commits
📁 rules	Rule updates			last month
📄 CVEs_red_team_tools.md	Update CVEs_red_team_tools.md			last month
📄 LICENSE.txt	Create LICENSE.txt			last month
📄 README.md	Update README.md			last month
📄 all-clam.ldb	add license to clam files			last month
📄 all-hashes.csv	Add files via upload			last month
📄 all-snort.rules	Rule updates			last month
📄 all-yara.yar	Rule updates			last month
📄 signatures_table_of_content.csv	Update signatures_table_of_content.csv			19 days ago

https://github.com/fireeye/red_team_tool_countermeasures

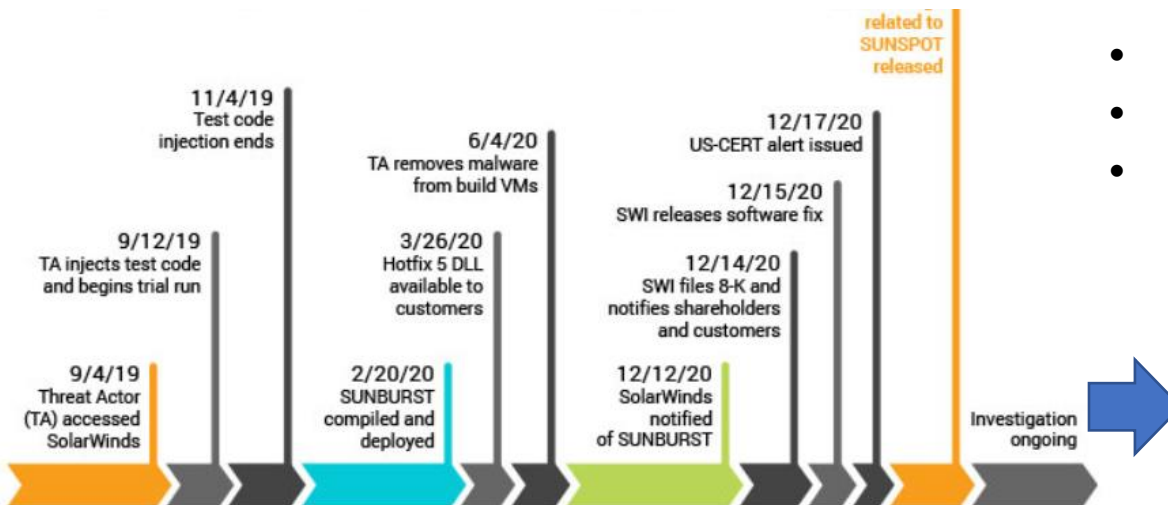
Then we went hit by... a Sunburst!



But, when we started realizing the attack against Fireeye, the entire Security community founded that a bigger plan was unfolding, a huge and highly sophisticated attack: SUNBURST.

Fireeye was just the last of a number of targets in a campaign initially led against Solarwinds, a Company developing a widely used network monitoring tool known as: Orion. In fact Orion was initially compromised to extend the attack to the rest of the targets.

SolarWinds was the victim of a cyberattack to our systems that inserted a vulnerability (SUNBURST) within our Orion® Platform software builds for versions **2019.4 HF 5, 2020.2 with no hotfix installed, and 2020.2 HF 1**, which, if present and activated, could potentially allow an attacker to compromise the server on which the Orion products run.



All events, dates, and times approximate and subject to change; pending completed investigation.

SolarWinds SUNBURST attack timeline, according to January 11, 2021, SolarWinds blog

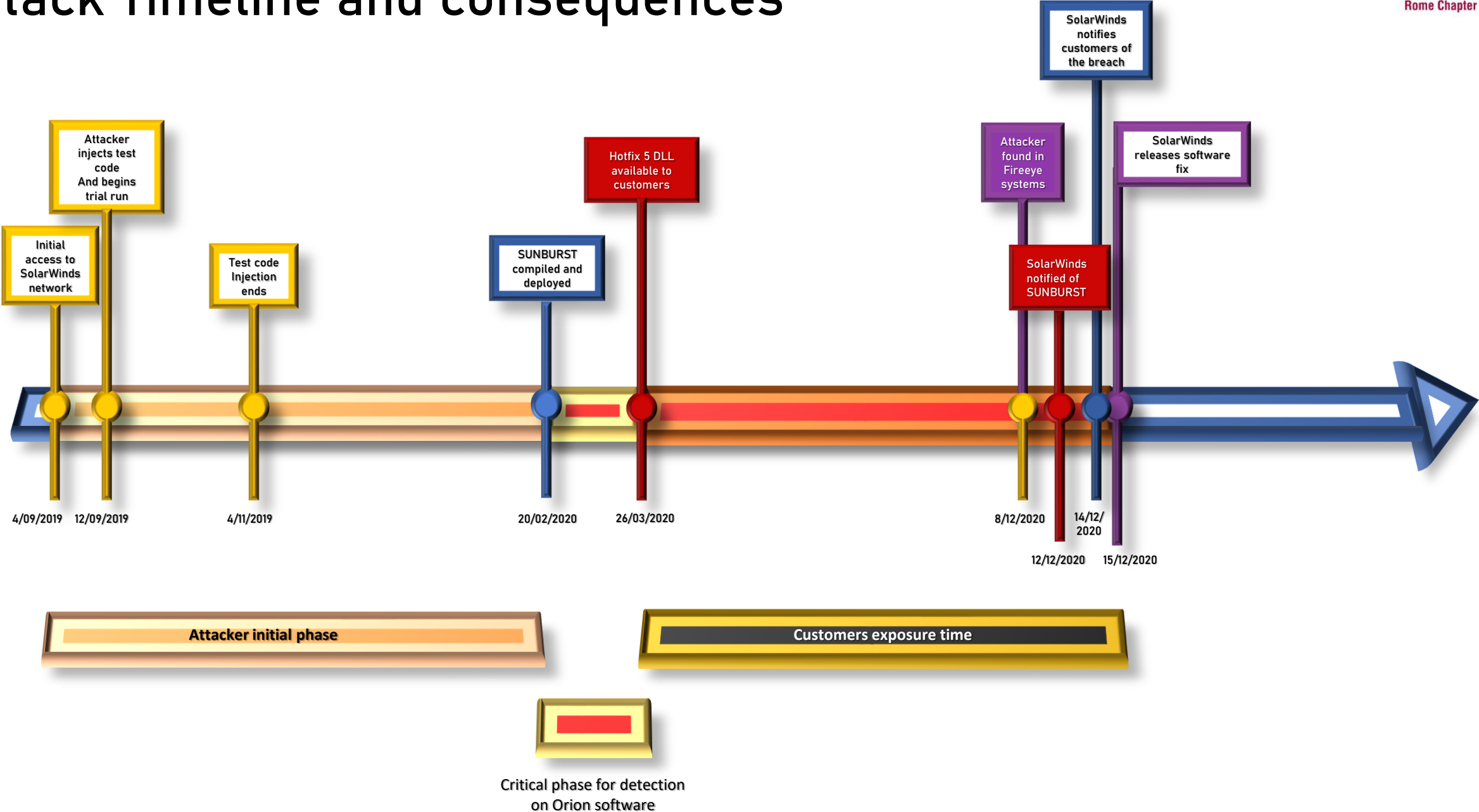
Courtesy of SolarWinds Inc.

- Sunburst is a “Supply-chain” attack.
- It is a global scale campaign.
- It is highly sophisticated.



The attacker injected a piece of malicious code in a specific SolarWinds Orion update compromising every system that went updated with it.

Attack Timeline and consequences



SUNBURST: some details...

These are the compromised releases of SolarWinds Orion:

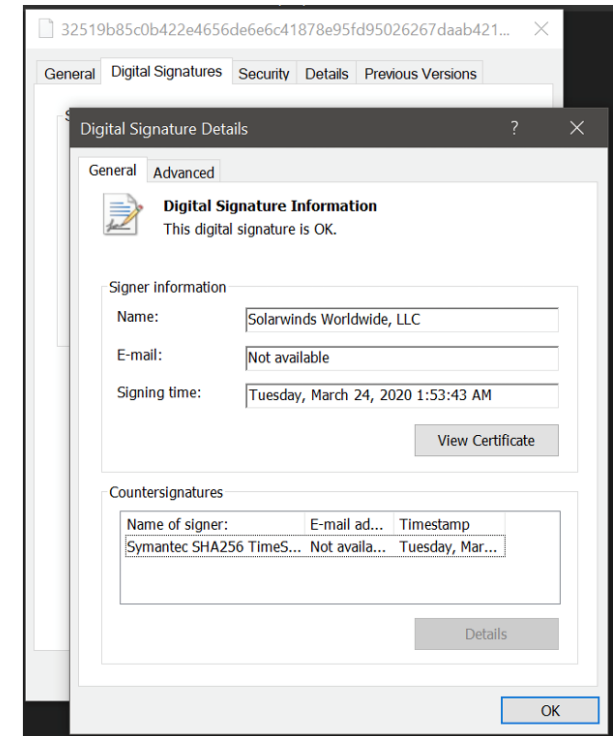
- Orion Platform 2019.4 HF5, version 2019.4.5200.9083
- Orion Platform 2020.2 RC1, version 2020.2.100.12219
- Orion Platform 2020.2 RC2, version 2020.2.5200.12394
- Orion Platform 2020.2, 2020.2 HF1, version 2020.2.5300.12432

Sunburst is a backdoor under the guise of a DLL:

- SolarWinds.Orion.Core.BusinessLayer.dll

It is signed by SolarWinds and the standard instructions for Orion setup recommend to put it and the other components in the system's whitelist.

Because of these reasons, the backdoor was facing very limited chances of being traced by Antivirus and HIPS/HIDS/EDR solutions. In addition, the backdoor itself included in its code a number of tricks to hide it from prying eyes...



SUNBURST: the other tools

Thanks to the initial Fireeye investigations, the SolarWinds breach unfolded very quickly and showed its magnitude.

In the Fireeye breach, as we learned with the successive investigations, the attacker used Sunburst as initial step and then resorted to installing other malware like CobaltStrike to move laterally extending his control upon the breached infrastructure.

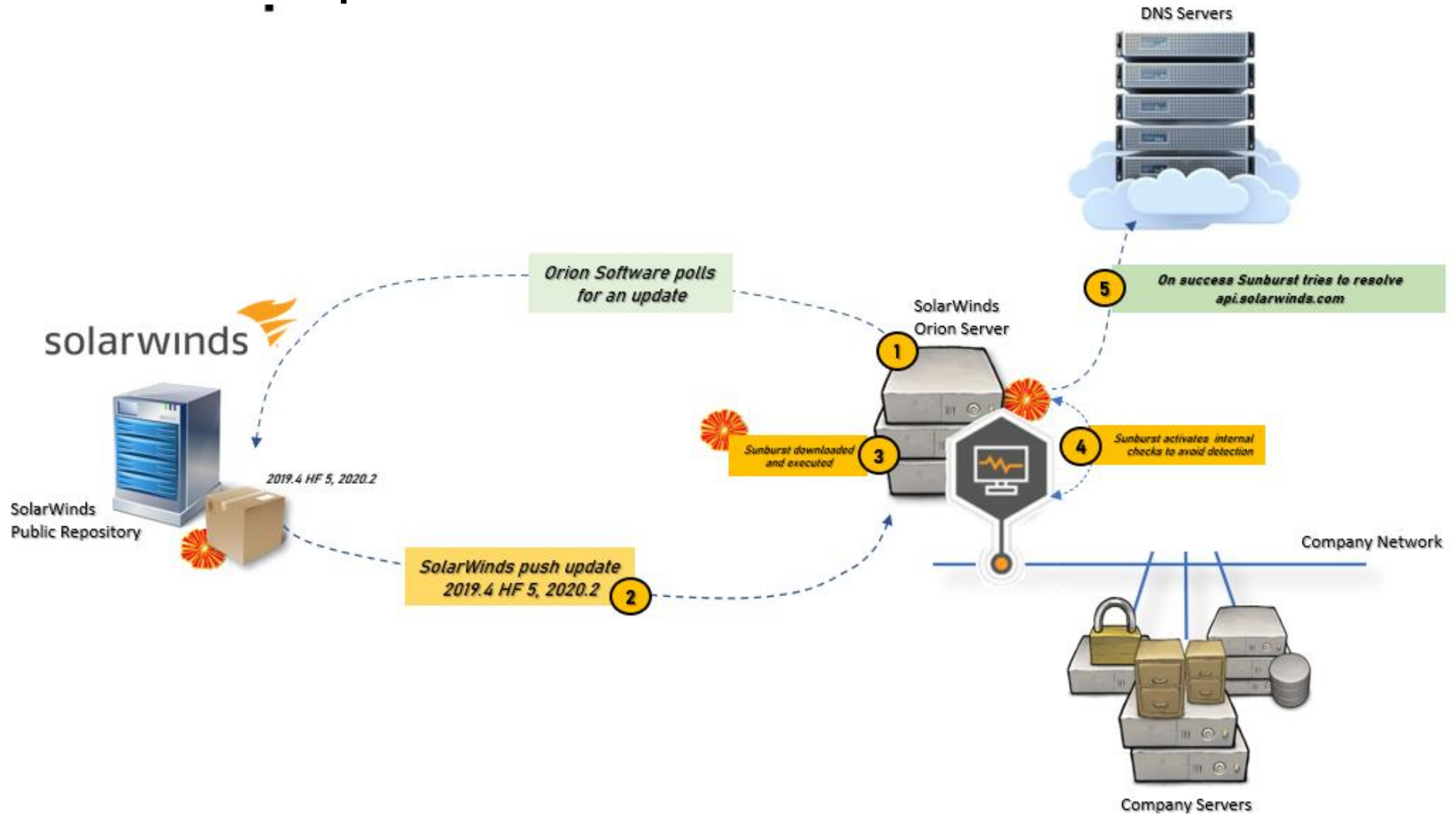
Collectively, the following malware families have been identified:

- Teardrop
- Raindrop
- Supernova
- CobaltStrike Agents (Beacons)

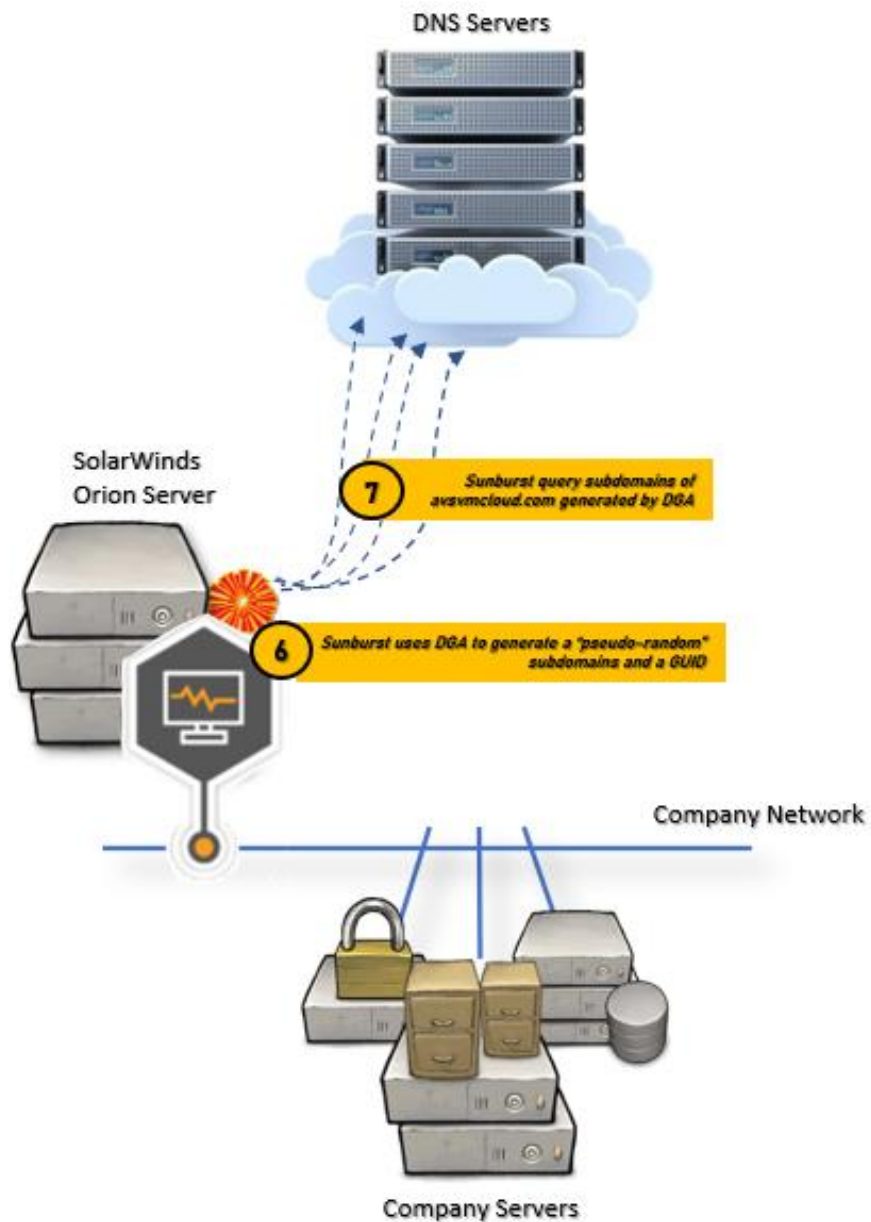
The background features a complex, abstract pattern of thin, light blue lines and small white dots. These elements are arranged in a way that creates a sense of depth and movement, resembling a network or a data visualization. The overall color palette is dominated by various shades of blue, with the text and logo providing white and red accents.

Let's go deeper

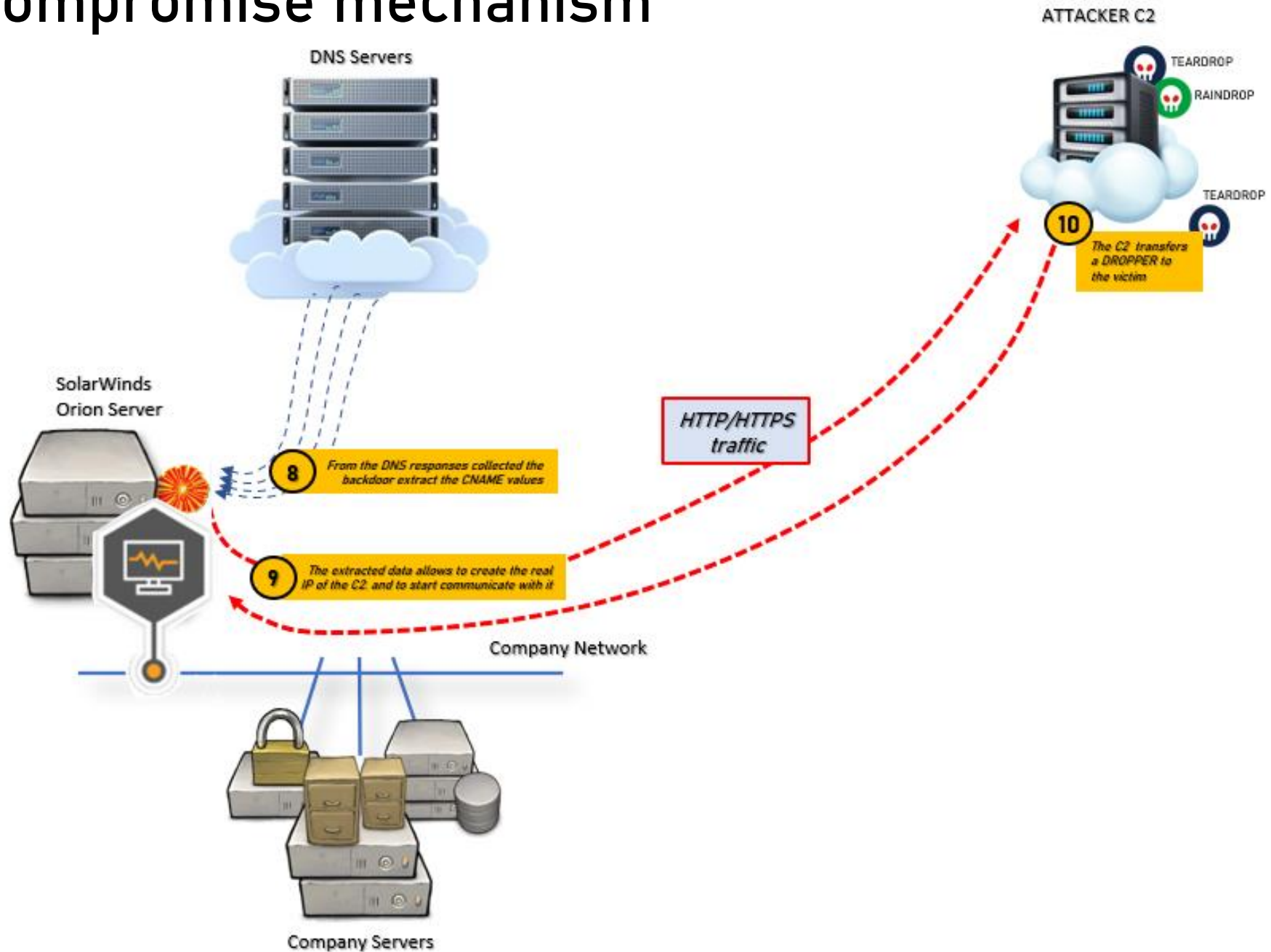
Sunburst: Compromise mechanism



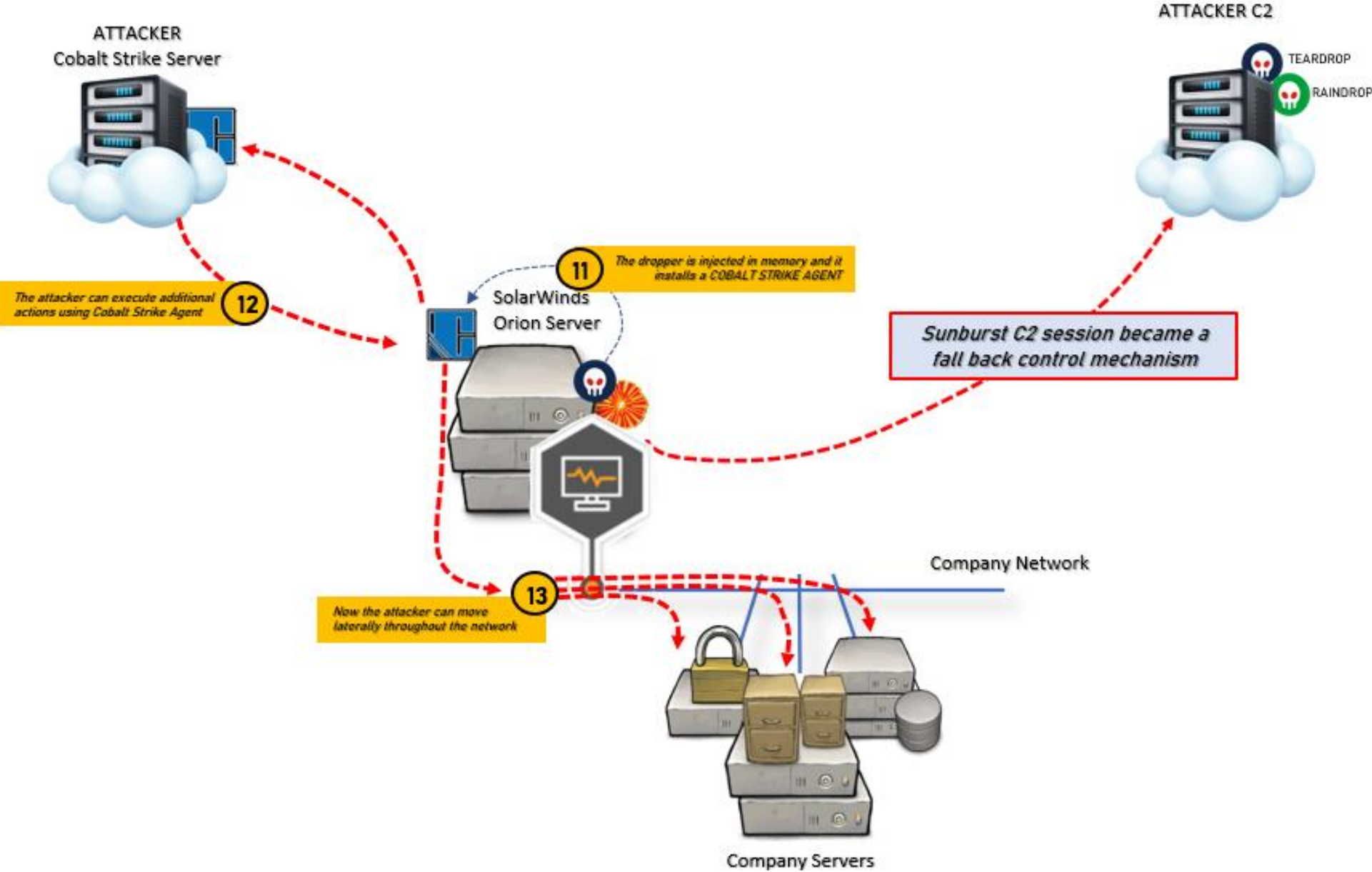
Sunburst: Compromise mechanism



Sunburst: Compromise mechanism



Sunburst: Compromise mechanism



SUNBURST: summary of its activation process.

Sunburst was directly downloadable from SolarWinds website as update of Orion Software.
At the end of the update process, once the main component is executed:

`SolarWinds.BusinessLayerHost.exe`

A number of plug-ins are loaded such as the DLL containing the backdoor:

`SolarWinds.Orion.Core.BusinessLayer.dll`

Inside, there is a class instanced:

`SolarWinds.Orion.Core.BusinessLayer.OrionImprovementBusinessLayer`

Which implements the backdoor.

The execution of the backdoor is carried out by the following routine:

`SolarWinds.Orion.Core.BusinessLayer.BackgroundInventory.InventoryManager.RefreshInternal`

connected with SolarWinds Inventory Manager of Orion, a component loaded as the program starts up.
The execution of the backdoor is tied with a number of initial controls integrated in the malware to protect it from potential discovery.

SUNBURST: evasion

Sunburst is a very sophisticated piece of malware with remarkable abilities to hide and protect itself.

When executed it performs several checks, the first is to verify if it has been launched on a machine inside the SolarWinds network. This check is made by verifying the hostname and Domain of the machine, against a set of predetermined hashes belonging to SolarWinds networks and compared at runtime.

```
private static readonly ulong[] patternHashes = new ulong[]
{
    // HASH                CRACKED                ASSUMPTIONS
    // -----
    1109067043404435916UL, // 'dev.local' => SolarWinds Dev local
    15267980678929160412UL, // 'swdev.dmz' => SolarWinds Development DMZ
    8381292265993977266UL, // 'lab.local' => Local lab
    3796405623695665524UL, // 'lab.na' => SolarWinds North America office
    4578480846255629462UL, // 'lab.brno' => SolarWinds Brno office
    8727477769544302060UL,
    10734127004244879770UL, // 'cork.lab' => SolarWinds Cork office
    11073283311104541690UL, // 'dev.local' => Development
    4030236413975199654UL, // 'dmz.local' => Demilitarized Zone
    7701683279824397773UL,
    5132256620104998637UL, // 'saas.swi' => maybe: SaaS SolarWinds
    5942282052525294911UL, // 'lab.rio' => maybe: SolarWinds Rio Office
    16858955978146406642UL // 'apac.lab' => SolarWinds APAC offices
};
```

This is the routine that call the list of Solarwinds networks stored as hashes.

```
if (array.Length >= 2)
{
    string s = array[array.Length - 2] + "." + array[array.Length - 1];
    foreach (ulong num in OrionImprovementBusinessLayer.patternHashes)
    {
        if (OrionImprovementBusinessLayer.GetHash(s) == num)
        {
            return true;
        }
    }
}
```

During the execution, the backdoor checks additional System variables (ANTIS) making the Dynamic Malware analysis via Sandbox unreliable.

While these checks are frequent in sophisticated malware, the number of them and the careful progression of their execution in one single backdoor is unlikely seen before.

SUNBURST: behavior...

To successfully integrate the malware in the Orion suite, the attacker has been forced to inject his code by altering legitimate functions.

For this reason, during the execution, the backdoor must interact with the following methods:

ReportWatcherRetry
ReportWatcherPostpone

These methods access an XML-like file called *appSettings* where Orion writes parameters to keep track of error at startup. These parameters are managed by, an API used to check the previous executions of Orion:

SolarWinds.Orion.Core.BusinessLayer.dll.config

These values are verified by the legitimate application during its initial execution cycle.

The backdoor, in the initial phase of Orion startup, uses these values as persistence parameters polled by `ReportWatcherRetry` key where the potential values can be anything from 1 to 4, but counting 3 as an exception that forced the backdoor activation routine to stop.

This highlights once more the sophistication of the attacker.

SUNBURST: technical considerations

The following SolarWinds components were affected by the attacker:

```
SolarWinds.Orion.Core.BusinessLayer.OrionImprovementBusinessLayer.Initialize  
SolarWinds.Orion.Core.BusinessLayer.BackgroundInventory.InventoryManager.RefreshInternal  
SolarWinds.Orion.Core.BusinessLayer.BackgroundInventory.InventoryManager.Refresh  
SolarWinds.Orion.Core.BusinessLayer.BackgroundInventory.InventoryManager.Start  
SolarWinds.Orion.Core.BusinessLayer.CoreBusinessLayerPlugin.ScheduleBackgroundInventory  
SolarWinds.Orion.Core.BusinessLayer.CoreBusinessLayerPlugin.Start
```

The malicious code was inserted in the “*RefreshInternal*” method and invoked upon execution by the main executable: “*SolarWinds.BusinessLayer.Host.exe*”.

This is another significant aspect to consider.

Instead of launching the backdoor through the canonical “*Start*” which results in immediate activation, increasing the chance of being detected, the attacker has bounded the malware with a necessary but subsequent process: the *refresh*, which runs with a significant delay.

Notably, if we consider how the method *RefreshInternal* is integrated in the backdoor execution flow, we can consider it “functional” not only to the delay of the backdoor execution but to the control of its status as well.

SUNBURST: behavior...

The activation checks are not over yet...

Once the status Report key check has been passed, the malware runs a query to enumerate the drivers loaded onto the System via a WMI query with this logic:

```
Select * From Win32_SystemDriver
```

The result is compared with a blacklist internal to the backdoor code where a number of drivers belonging to Security solutions such as Antivirus and EDRs is stored, decrypted at runtime.

In presence of a Security driver installed, the appSettings XML file is updated with a value of 4, a backdoor routine modifies the registry key of the driver unloading it and the backdoor setup exits without errors.

This postpone the activation to a subsequent launch of Orion, but more importantly, on the next setup, the «hostile» Security driver will be not active.

Instead, on successful check of System drivers, the backdoor setup is completed and the malware will check Internet by querying the DNS resolution of :

```
api.solarwinds.com
```

SUNBURST: Evasion

This is the entire list of controls carried out by backdoor prior to activate itself onto a system:

Sequence	Detection mechanism
1	Determine the current load malicious by hash DLL The name of the process is solarwinds.businesslayerhost.exe
2	The malicious DLL checks its last write time against the current time and verifies the amount of time passed. It means that it will be dormant for about half a month before implementation.
3	Check hard coded named pipe: 583da945-62af-10e8-4902-a8f205c72b2e. This avoids repeated execution of multiple processes of the same backdoor.
4	Check configuration options for malicious reuse ReportWatcherRetry, ReportStatus Item cannot be 3, namely Truncate Exit state is matched forcing the execution to exit.
5	Check the domain of the current device. The domain name is compared against a blacklist of domains saved as hardcoded hashes in the backdoor. The domain name cannot match the regular expression "(?i)([^a-z]^)(test)([^a-z] \$)". This expression is mainly used to check whether the current domain name is the domain name for testing ;"(?i)(solarwinds)". This means the malware detect whether it is executed inside Solarwinds offices and exit execution.
6	Check the first non loopback enabled NIC , be not in IP Blacklist.
7	Detection process Hash. The blacklist (contain about 137 processes), ensure that there are no security related software and services in the current environment , such as : Windbg, Autoruns, Wireshark, etc... and try to close the service in the service list
8	Check if there is a driver for security applications such as : groundling32.sys
9	It checks the availability of "api.solarwinds.com" to proceed to communicate with its C2s.

SUNBURST: Network checks

Through the setup process, Sunburst will generate an A DNS record, that will be checked against a blacklist of addresses encoded in its configuration and illustrated below:

10.0.0.0/8
172.16.0.0/12
192.168.0.0/16
224.0.0.0/3
fc00:: - fe00::
fec0:: - ffc0::
ff00:: - ff00::
20.140.0.0/15
96.31.172.0/24
131.228.12.0/22
144.86.226.0/24

*Microsoft
IP address spaces*

The presence of a match terminates immediately the backdoor process and a key with value of 3 will be saved in a Orion configuration XML file by polling a Orion watcher:

ReportWatcherRetry

This value (3) will block any further activation of the backdoor. This value is checked at the beginning of any backdoor setup process.

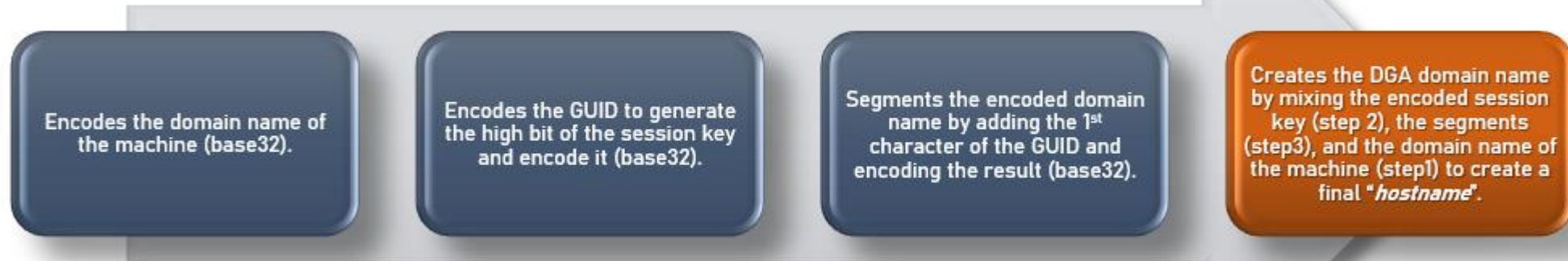
If the check return no matches, a new thread will be launched calling:

HttpHelper.Initialize

Activating the DGA and preparing for the C2 communication.

SUNBURST: DGA...

Sunburst leverages on DGA (Domain Generation Algorithm) to communicate with its C2. During the setup, the backdoor applies the DGA to generate the hostname, a unique identified that will be used to check to its C2. To do that it goes through these steps:



Once the fourth step is completed, the hostname will be added to four DNS records generated by DGA. The DNS records will include the Domain and will be composed by the following structure:

```
${GUID:16byte}${Encoded_AD_domain}.appsync-api.${region}.avsvmcloud.com
```

The "region" field has the following values:

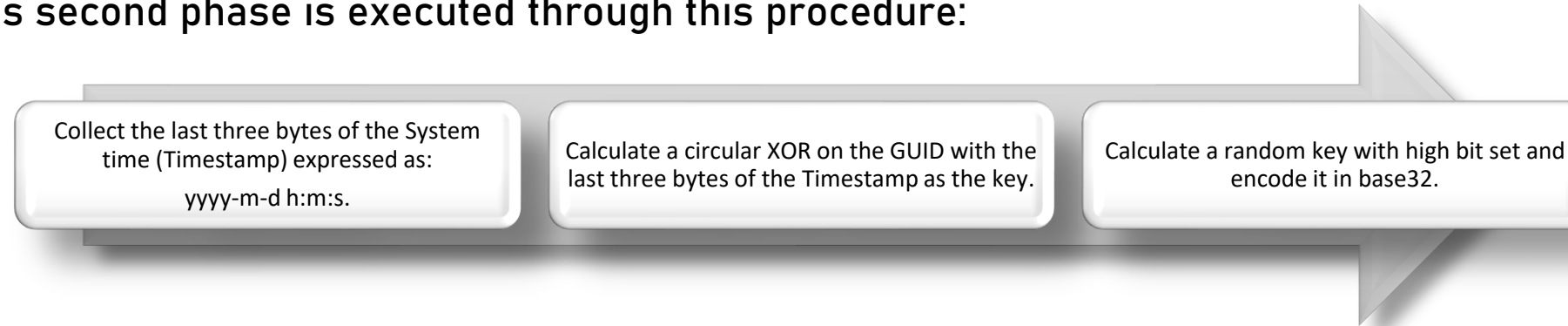
```
eu-west-1  
us-west-2  
us-east-1  
us-east-2
```

The result is:

```
.appsync-api.eu-west-1.avsvmcloud.com  
.appsync-api.us-west-2.avsvmcloud.com  
.appsync-api.us-east-1.avsvmcloud.com  
.appsync-api.us-east-2.avsvmcloud.com
```

SUNBURST: DGA...

- By analyzing the DNS traffic we noticed that Sunburst is not utilizing the TXT record in a manner traditionally seen in other DNS tunneling tools or other malware such as Necurs.
- It uses the CNAME record and an efficient steganography, again to overcome the traditional network forensics and packet inspection solutions.
- In addition, the backdoor is using the DGA in two distinctive phases.
 - In the first phase it creates the pseudo-random subdomain,
 - in the second phase it uses the method *GetNextString* to finalize the communication with its C2.This second phase is executed through this procedure:



- The DGA Domain name generated is split into four random names and a DNS query is sent.
- The result of the query is compared again with the black and whitelists and, upon a successful check, the CNAME and the VALUE (IP Address field) of the response will be tagged as “*ext*”, thereby transitioning to the next phase.

SUNBURST: details...

The communication routine of Sunburst is based on DGA (Domain Generation Algorithm) and every victim has its own subdomains (based on internal names) that, once encoded, are unique.

Decoded Internal Nam	Possible Organization (may be inaccur	Type of mess	First Seen
corp.stratusnet	Stratus Networks	2nd stage	17/04/2020
resprod.com	Res Group (Renewable energy company)	2nd stage	06/05/2020
te.nz	TE Connectivity (Sensor manufacturer)	2nd stage	13/05/2020
fidelitycomm.io	Fidelity Communications (ISP)	2nd stage	02/06/2020
corp.stingraydi	Stingray (Media and entertainment)	2nd stage	03/06/2020
nswhealth.net	NSW Health	2nd stage	12/06/2020
corp.ptci.com	Pioneer Telephone Scholarship Recipients	2nd stage	19/06/2020
digitalsense.co	Digital Sense (Cloud Services)	2nd stage	24/06/2020
ggsg-us.cisco	Cisco GGSG	2nd stage	24/06/2020
mountsinai.hosp	Mount Sinai Hospital	2nd stage	02/07/2020
pqcorp.com	PQ Corporation	2nd stage	02/07/2020
mountsinai.hospital	Mount Sinai Hospital, New York	2nd stage	02/07/2020
kcpl.com	Kansas City Power and Light Company	2nd stage	07/07/2020
sm-group.local	SM Group (Distribution)	2nd stage	07/07/2020
pcsko.com	Professional Computer Systems	2nd stage	23/07/2020
itps.uk.net	ITPS (IT Services)	2nd stage	11/08/2020
ad001.mtk.io	Mediatek	2nd stage	26/08/2020
netdecisions.io	Netdecisions (IT services)	2nd stage	04/10/2020
mixonhill.com	Mixon Hill (intelligent transportation systems)	Terminate	29/04/2020
ies.com	IES Communications	Terminate	11/06/2020
ansc.gob.pe	GOB (Digital Platform of the Peruvian State)	Terminate	25/07/2020
insead.org	INSEAD Business School	Terminate	07/11/2020
xnet.kz	X NET (IT provider in Kazakhstan)	Unknown	09/06/2020
us.deloitte.co	Deloitte	Unknown	08/07/2020
e-idsolutions.	IDSolutions (video conferencing)	Unknown	16/07/2020
ad.optimizely.	Optimizely, Software Company	N/A	N/A
aerioncorp.com	Aerion Corporation	N/A	N/A
belkin.com	Belkin International	N/A	N/A
cisco.com	Cisco	N/A	N/A
corp.sana.com	Sana Biotechnology	N/A	N/A
int.lukoil-international.uz	Lukoil	N/A	N/A
neophotonics.co	NeoPhotonics Corporation	N/A	N/A
nvidia.com	Nvidia	N/A	N/A
vantagedatacenters.local	Vantage Data Centers	N/A	N/A
voceracommunications.com	Vocera Communications	N/A	N/A

If we decrypt the Internal names, we can notice the magnitude of the attack and some of its victims:

- *Department of Agriculture*
- *Department of Commerce*
- *Department of Defense*
- *Department of Energy*
- *Department of Health and Human Services*
- *Department of Homeland Security*
- *Department of Justice*
- *Department of State*
- *Department of the Treasury*
- *Administrative Office of the United States Courts*

Per approfondimenti:

https://github.com/RedDrip7/SunBurst_DGA_Decode

<https://github.com/bambenek/research/tree/main/sunburst>

<https://twitter.com/RedDrip7>

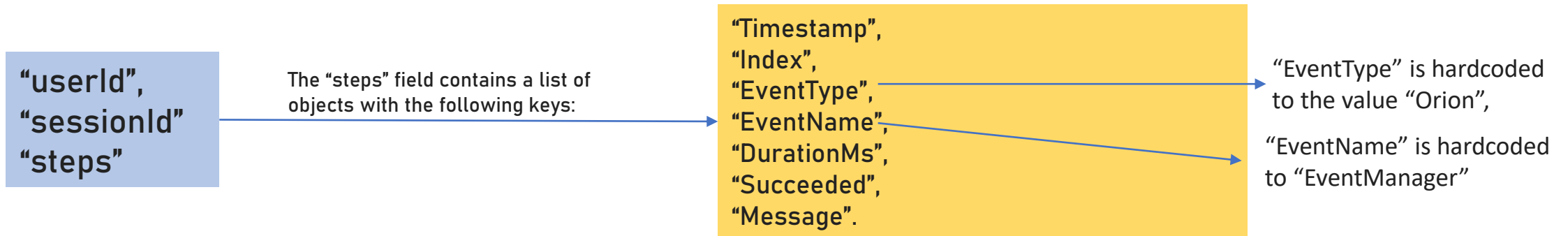
SUNBURST: Network Command and Control (C2)

Once the backdoor is actively managed, the attacker leverages on HTTP/HTTPs protocol. This type of traffic is started with a delay, coded into the malware (minimum 60 seconds) to fool any network monitoring tool.

From the pure traffic perspective the malware uses HTTP GETs, POSTs and PUTs:

The HTTP GET header «content-type» is configured as "application/octet-stream"
The HTTP POST header «content-type» is configured as "application/json"

The POST JSON payload contains peculiar keys and some are designed to fool the network monitoring:



Malware response messages sent to the server are DEFLATE compressed and single-byte-XOR encoded, then split among the "Message" fields in the "steps" array. Each "Message" value is Base64 encoded separately.

SUNBURST backdoor parameters

Command	Value	Operation
Idle	0	No operation
Exit	1	Terminate the current thread.
SetTime	2	Sets the delay time between main event loop executions Delay is in seconds, and varies random between $[.9 * <delay>, 1.1 * <delay>]$. If the delay is < 300 it is doubled on the next execution through the loop, this means it should settle onto an interval of around [5, 10] minutes. There is a second, unrelated delay routine that delays for a random interval between [16hrs, 83hrs]
CollectSystemDescription	3	Profile the local system including hostname, username, OS version, MAC addresses, IP address, DHCP configuration, and domain information.
UploadSystemDescription	4	Perform a HTTP request to the specified URL, parse the results and compare components against unknown hashed values. Format a report and send to the C2 server.
RunTask	5	Starts a new process with the given file path and arguments
GetProcessByDescription	6	Returns a process listing. If no arguments are provided returns just the PID and process name. If an argument is provided it also returns the parent PID and username and domain for the process owner.
KillTask	7	Terminate the given process, by PID.
GetFileSystemEntries	8	Given a path and an optional match pattern recursively list files and directories
WriteFile	9	Given a file path and a Base64 encoded string write the contents of the Base64 decoded string to the given file path. Write using append mode. Delay for [1s, 2s] after writing is done.
FileExists	10	Tests whether the given file path exists.
DeleteFile	11	Deletes the specified file path.
GetFileHash	12	Compute the MD5 of a file at a given path and return result as a HEX string. If an argument is provided, it is the expected MD5 hash of the file and returns an error if the calculated MD5 differs.
ReadRegistryValue	13	Arbitrary registry read from one of the supported hives
SetRegistryValue	14	Arbitrary registry write from one of the supported hives.
DeleteRegistryValue	15	Arbitrary registry delete from one of the supported hives
GetRegistrySubKeyAndValueNames	16	Returns listing of subkeys and value names beneath the given registry path
Reboot	17	Attempts to immediately trigger a system reboot.

SUNBURST: technical considerations

- In general, from the pure technical explanation of the commercial software compiling mechanism, any backdoored DLL would be identified during the commit phase and the subsequent automatic code review stage if the attacker were not able to access and modify the source code.
- In addition, as we will present later, the malicious DLL is not just included in the software bundle, but it is linked with other components, thus further confirming the hypothesis.
- In fact, to modify a piece of code or swap one DLL with another, is not enough for the backdoor to work, the attacker was also forced to link it with other components, and that is possible only by accessing these other components as well.
- As a blog on Reversing Lab analysis confirmed¹, the timestamps between the different components of the SolarWinds suite are all aligned due to being controlled by a remote server that is outside of the build environment that cannot be tampered with; this confirms the hypotheses about the access to the development area by the attacker.
- For additional details and a complete review of the tools used in this attack you can read my white paper posted on the RSA blog:

<https://community.rsa.com/t5/rsa-netwitness-platform-blog/sunburst-solorigate-round-up/ba-p/594084>

¹ <https://blog.reversinglabs.com/blog/sunburst-the-next-level-of-stealth>

Let's now check the other tools

The other tools: TEARDROP

TEARDROP, as its name anticipates, is a DLL dropper: a “Second Stage” which allows the attacker to introduce additional malware, specifically CobaltStrike agents. TEARDROP can be executed as a Service or at runtime.

- TEARDROP was found tightly connected with SUNBURST backdoor.
- Usually, in backdoored systems, the second stage was always TEARDROP.

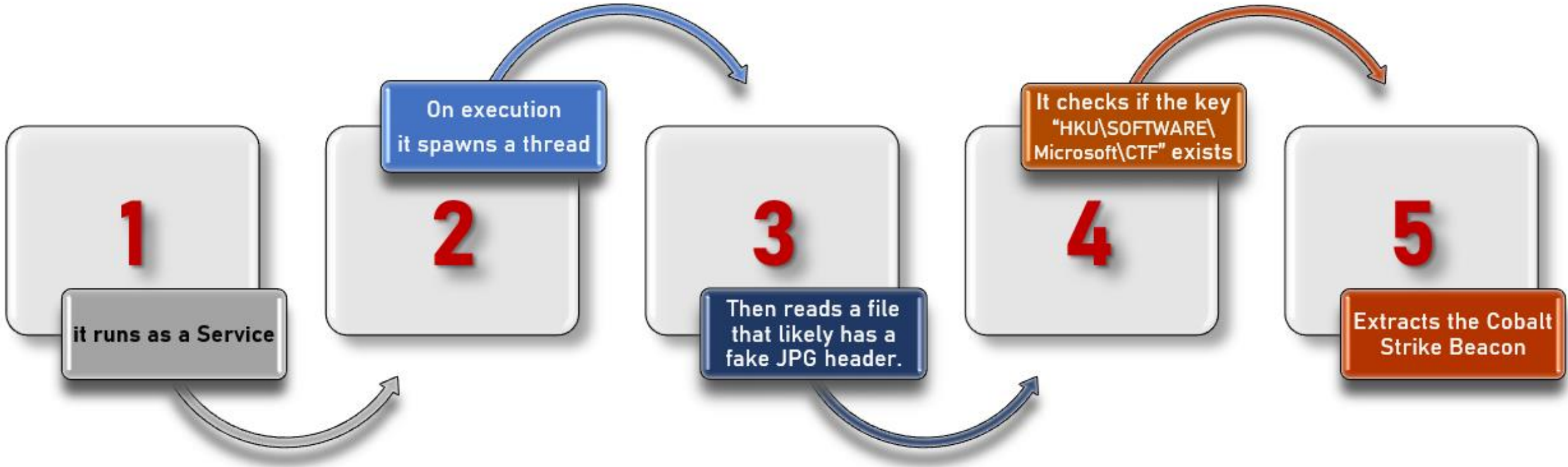
During execution, the dropper spawns a thread and read a fake “.jpg” file before continuing the setup. Technically, TEARDROP is not planned to carry out controls upon its running environment, as Sunburst does. It is a simple Loader storing an encrypted PE payload that, when detonated, is loaded in memory. The PE payload is a customized CobaltStrike agent that will beacon to specific domains such as:

- infinitysoftwares[.]com

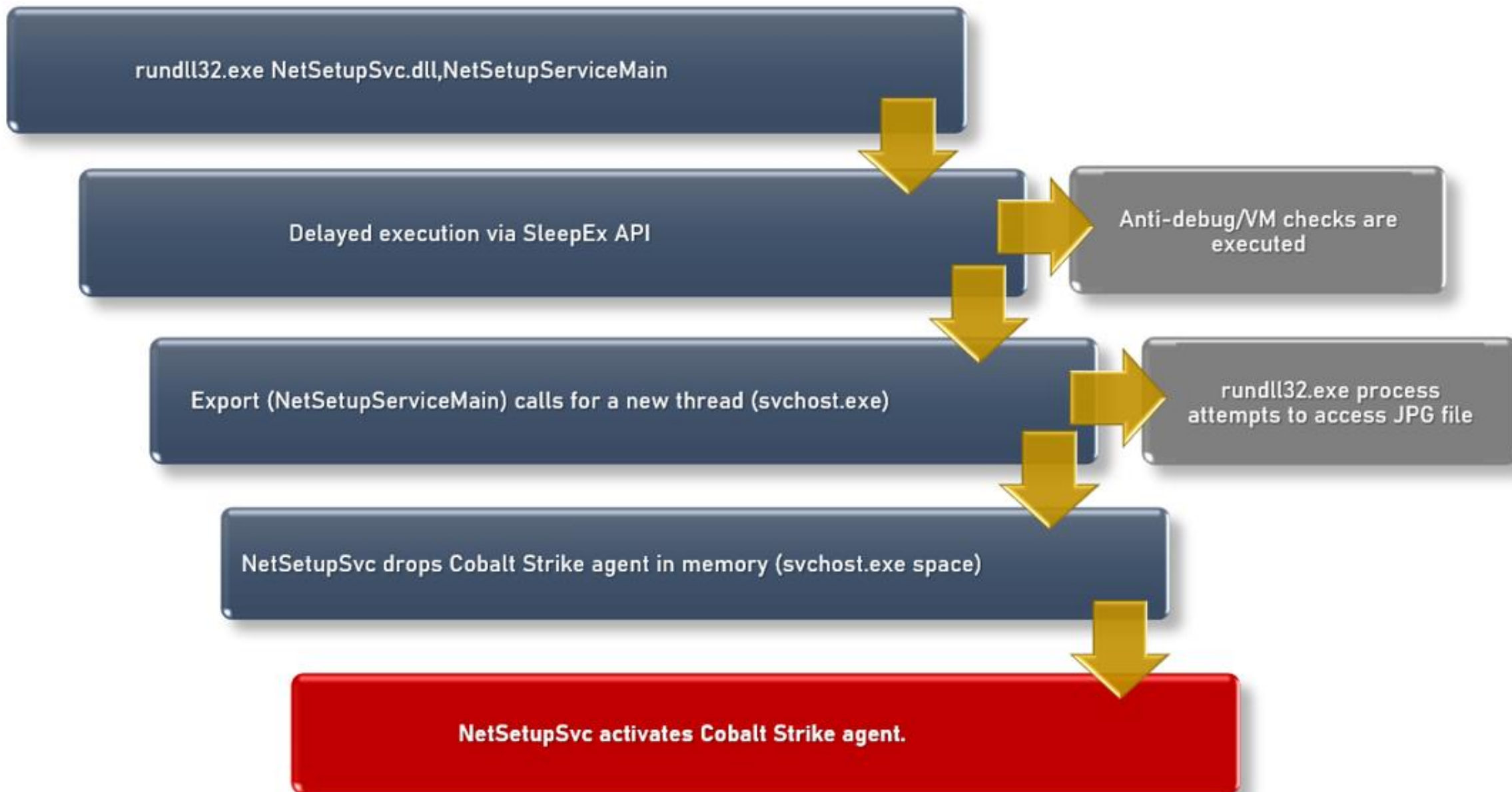
Notably:

- the TEARDROP samples collected so far are not signed with a certificate.

TEARDROP: activation mechanism



TEARDROP: CobaltStrike agent drop



The other tools: RAINDROP

RAINDROP is another dropper used to disseminate CobaltStrike agents in the Sunburst campaign.

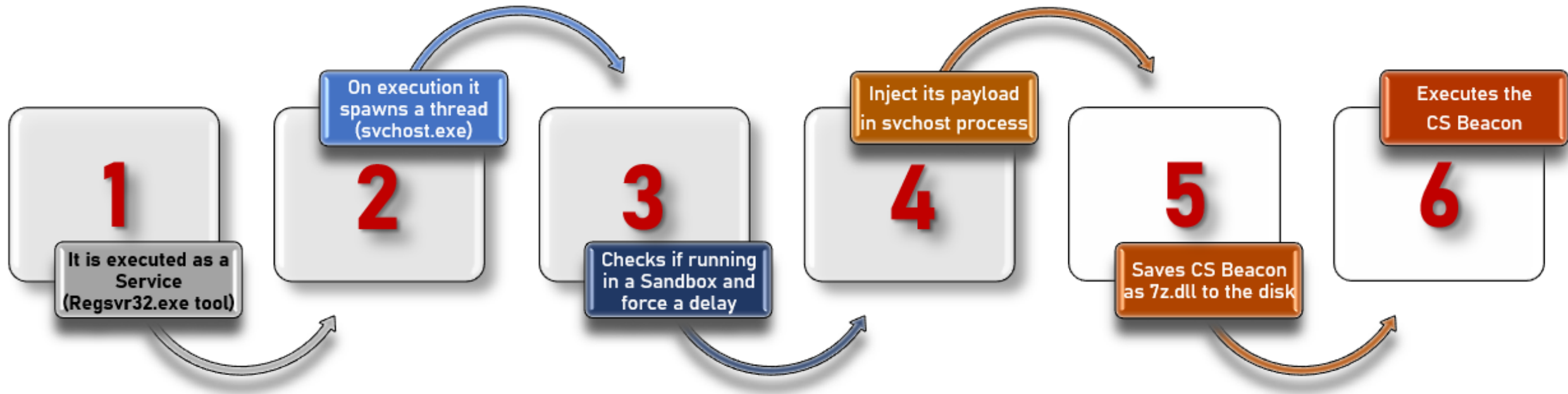
RAINDROP has some similarities with TEARDROP in terms of behaviors during its execution. However significant differences can be highlighted:

- In systems showing the presence of RAINDROP we didn't find SUNBURST installed, while instead it was present where we traced TEARDROP.
- RAINDROP uses a different packer to encrypt its payload.

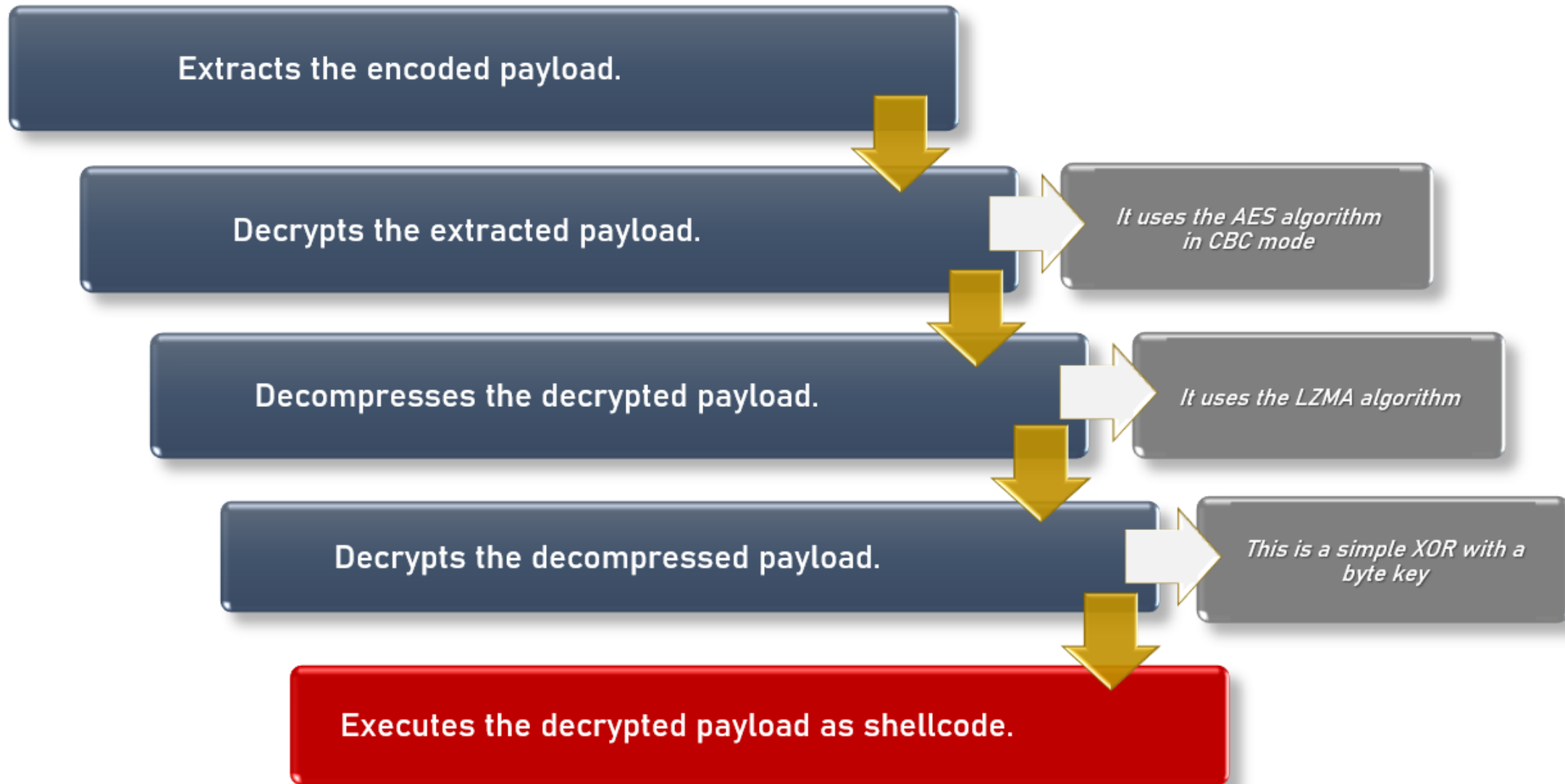
RAINDROP is a DLL created from the source code of 7-zip, but it never executes 7-zip routines. Upon execution, RAINDROP spawns a new thread, drops its payload and executes it. At runtime it execute the following steps:

- It delays the immediate activation of its functions by calling additional tasks.
 - Extract its payload (encrypted with AES in CBC mode).
 - Decompress the payload (with LZMA compression algorithm).
 - Decrypts its payload (XOR with byte key).
 - Launch the payload in memory.
- RAINDROP samples are not signed with a certificate.

RAINDROP: activation mechanism



RAINDROP: CobaltStrike agent drop



TEARDROP and CobaltStrike:

Looking to the third-phase of any Sunburst/Solorigate attack, we face now CobaltStrike agents.

These agents different for any infection, but they are showing some common traits:

- The agents are never installed by Sunburst backdoor, but deployed using TEARDROP or RAINDROP.
- They are written into a legitimate-looking subfolder in *%WinDir%* (e.g., *C:\Windows*)
- They are keeping persistence on a victim using a separate technique leveraging on a VBS script.
- They are generated using Artifact Kit templates of CobaltStrike as demonstrated by Checkpoint and Microsoft analyses.

```

sub_41605 proc near
var_48= qword ptr -48h
sub     rsp, 68h
call   cs:GetTickCount
mov     ecx, 26AAh
xor     edx, edx
mov     r9d, 5Ch ; '\
div     ecx
lea     rcx, Buffer
mov     r8d, 5Ch ; '\
mov     dword ptr [rsp+68h+var_48+30h], 5Ch ; '\
mov     dword ptr [rsp+68h+var_48+28h], 65h ; 'e
mov     dword ptr [rsp+68h+var_48+20h], 70h ; 'p
mov     dword ptr [rsp+68h+var_48+18h], 69h ; 'i
mov     dword ptr [rsp+68h+var_48+10h], 70h ; 'p
mov     dword ptr [rsp+68h+var_48+8], 5Ch ; '\
mov     dword ptr [rsp+68h+var_48], 2Eh ; '.'
mov     dword ptr [rsp+68h+var_48+38h], edx
lea     rdx, byte_86000
call   j_sprintf
lea     r8, sub_414F5
xor     ecx, ecx
mov     [rsp+68h+var_48+8], 0
mov     dword ptr [rsp+68h+var_48], 0
xor     r9d, r9d
xor     edx, edx
call   cs:CreateThread
xor     ecx, ecx
add     rsp, 68h
jmp     sub_415B2
sub_41605 endp

```

Teardrop's BEACON

```

sub_6BAC1605 proc near
dwCreationFlags= dword ptr -48h
lpThreadId= qword ptr -40h
var_38= dword ptr -38h
var_30= dword ptr -30h
var_28= dword ptr -28h
var_20= dword ptr -20h
var_18= dword ptr -18h
var_10= dword ptr -10h
sub     rsp, 68h
call   cs:GetTickCount
mov     ecx, 26AAh
xor     edx, edx
mov     r9d, 5Ch ; '\
div     ecx
lea     rcx, Buffer ; Buffer
mov     r8d, 5Ch ; '\
mov     [rsp+68h+var_18], 5Ch ; '\
mov     [rsp+68h+var_20], 65h ; 'e
mov     [rsp+68h+var_28], 70h ; 'p
mov     [rsp+68h+var_30], 69h ; 'i
mov     [rsp+68h+var_38], 70h ; 'p
mov     dword ptr [rsp+68h+lpThreadId], 5Ch ; '\
mov     [rsp+68h+dwCreationFlags], 2Eh ; '.'
mov     [rsp+68h+var_10], edx
lea     rdx, Format ; "%c%c%c%c%c%c%c%c%MSSE-%d-server"
call   sprintf
lea     r8, StartAddress ; lpStartAddress
xor     ecx, ecx ; lpThreadAttributes
mov     [rsp+68h+lpThreadId], 0 ; lpThreadId
mov     [rsp+68h+dwCreationFlags], 0 ; dwCreationFlags
xor     r9d, r9d ; lpParameter
xor     edx, edx ; dwStackSize
call   cs:CreateThread
xor     ecx, ecx
add     rsp, 68h
jmp     sub_6BAC15B2
sub_6BAC1605 endp

```

CobaltStrike's BEACON

The other tools: SUPERNOVA

SUPERNOVA is an .NET webshell developed from a legitimate SolarWinds Orion DLL.

- SUPERNOVA executable is not signed

The modification carried out upon the original DLL is simple, but extremely effective.

Adding the method `DynamicRun()` in the class `LogImageHandler` the attacker was able to transform an harmless DLL into a sophisticated webshell.

The injected method is processed by the HTTP routine managing the requests to the FrontEnd of the SolarWinds application, it allows the attacker to pass parameters mimicking an HTTP request.

Thanks to this trick, it is possible for the attacker to pass a block of C# code and ensure its execution when intercepted by `DynamicRun`, which in turn will pass it to `CSharpCodeProvider`, a .NET class used to compile code at runtime in memory.

- SUPERNOVA do not abuses vulnerabilities, but structural weaknesses of .NET environment making it difficult to be spotted with a generic analysis.

SUPERNOVA differs from Sunburst on significant aspects:

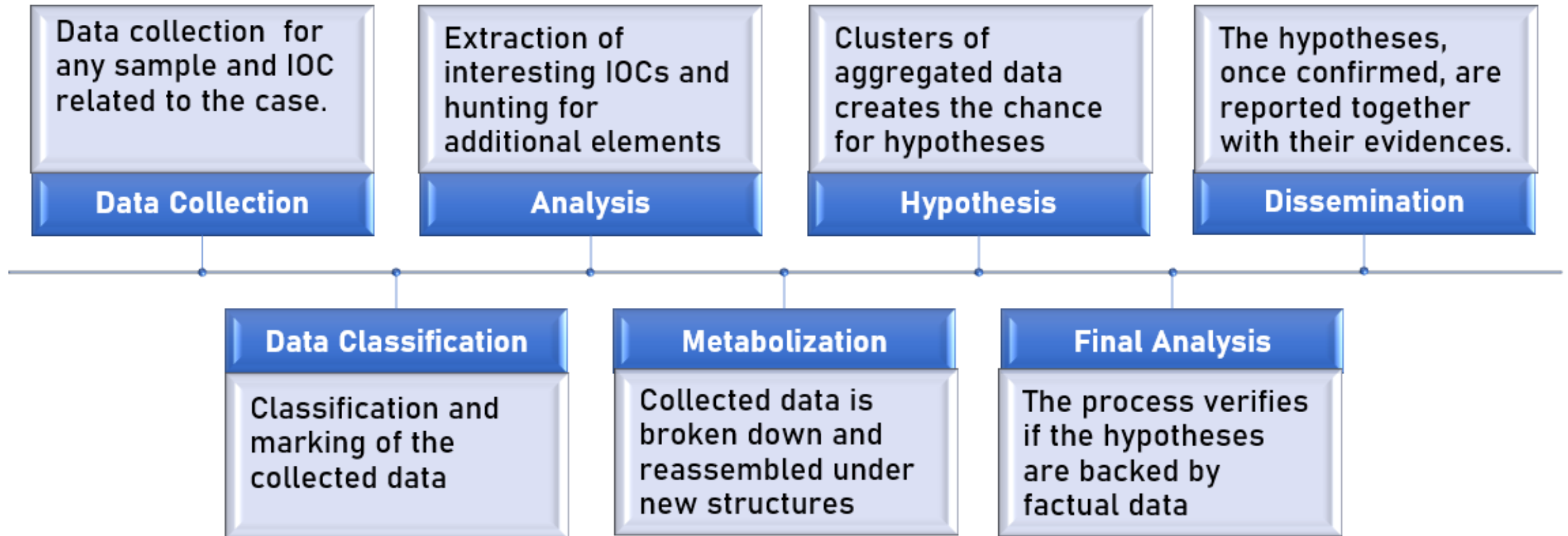
- SUPERNOVA code is simple compared to Sunburst code
- SUPERNOVA implant was not included in the Orion release, but instead added by an intruder after its initial attack.

Sunburst: Threat Intel

Our Threat Intel process

Our general Threat Intel approach is based on a set of steps illustrated below.

The analysis begins from the known IOCs and aims to develop a bigger set of indicators, building hypotheses during the process, but only in presence of factual evidences, and to compose the narrative of the incident to build a precise Report.



Analysis

Collection, Classification & Analysis

- We started the task by collecting initial details of the breach from OSINT and enriched it with the outcome of our Team IR analyses.
- The collection task was divided in four main areas:
 - Malware IOCs
 - Network IOCs
 - Attacking Techniques
 - Registrant analysis
- The classification associated each IOC to one or more clusters aiming to differentiate and evaluate the data both as a whole and for its specific informational value. Under this process, another important parameter was the “level of trust” of each IOC (the reliability of the IOC and the source who extracted it).
- The analysis aimed to evaluate the clusters and expand the hypotheses formulated starting with them to confirm or dismiss one or more data conglomerates and to apply logic to clarify the confirmed hypotheses.
- The analysis is still ongoing, as we collect additional IOCs recently and because the Threat Intel is a continuous process.
- However, we are also wrapping up a report that would be released as a white paper by RSA about the outcome of this investigation.

Registrar and Hosting providers

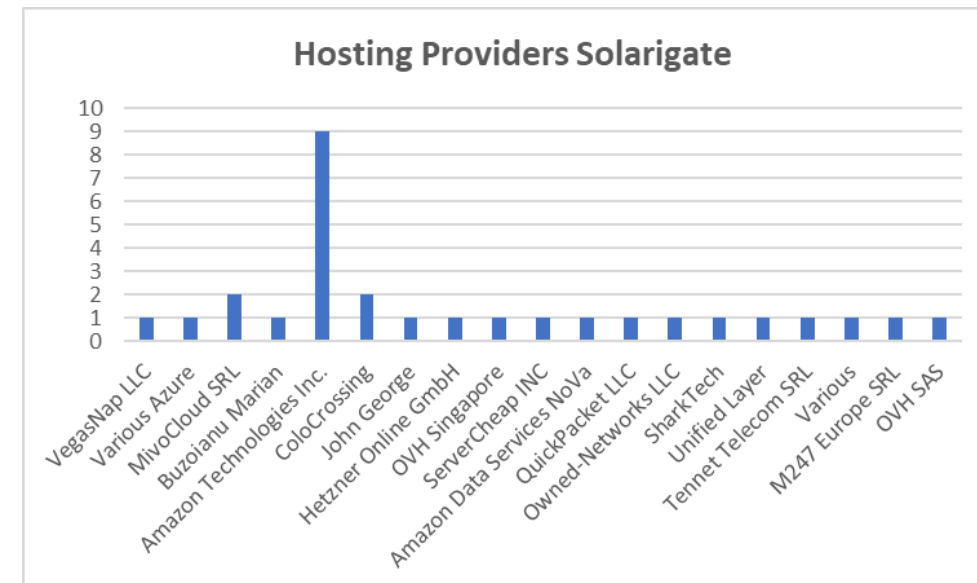
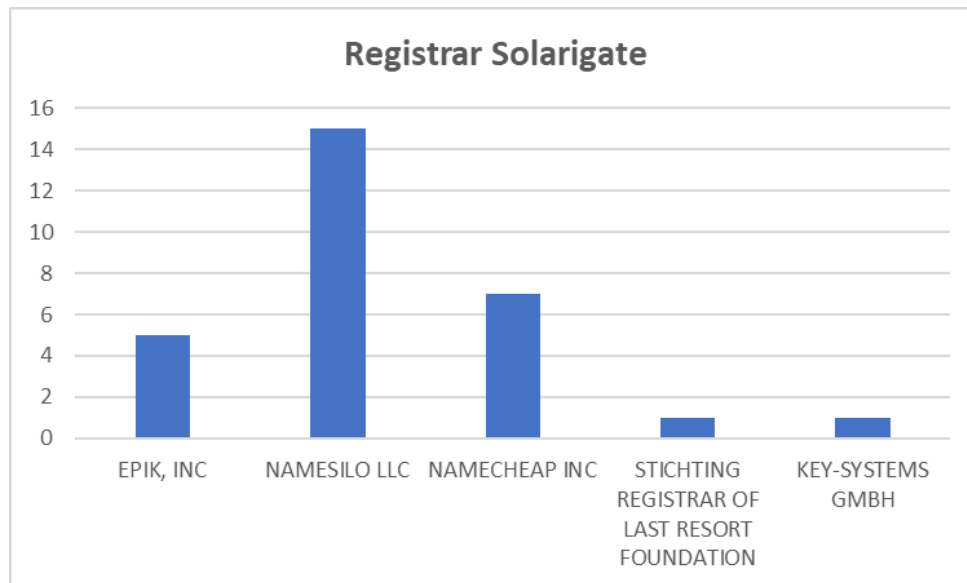
1# NETWORK IOCS ANALYSIS

Registrars Analysis

One of the more interesting field of analysis, in Sunburst, is the Registrars.

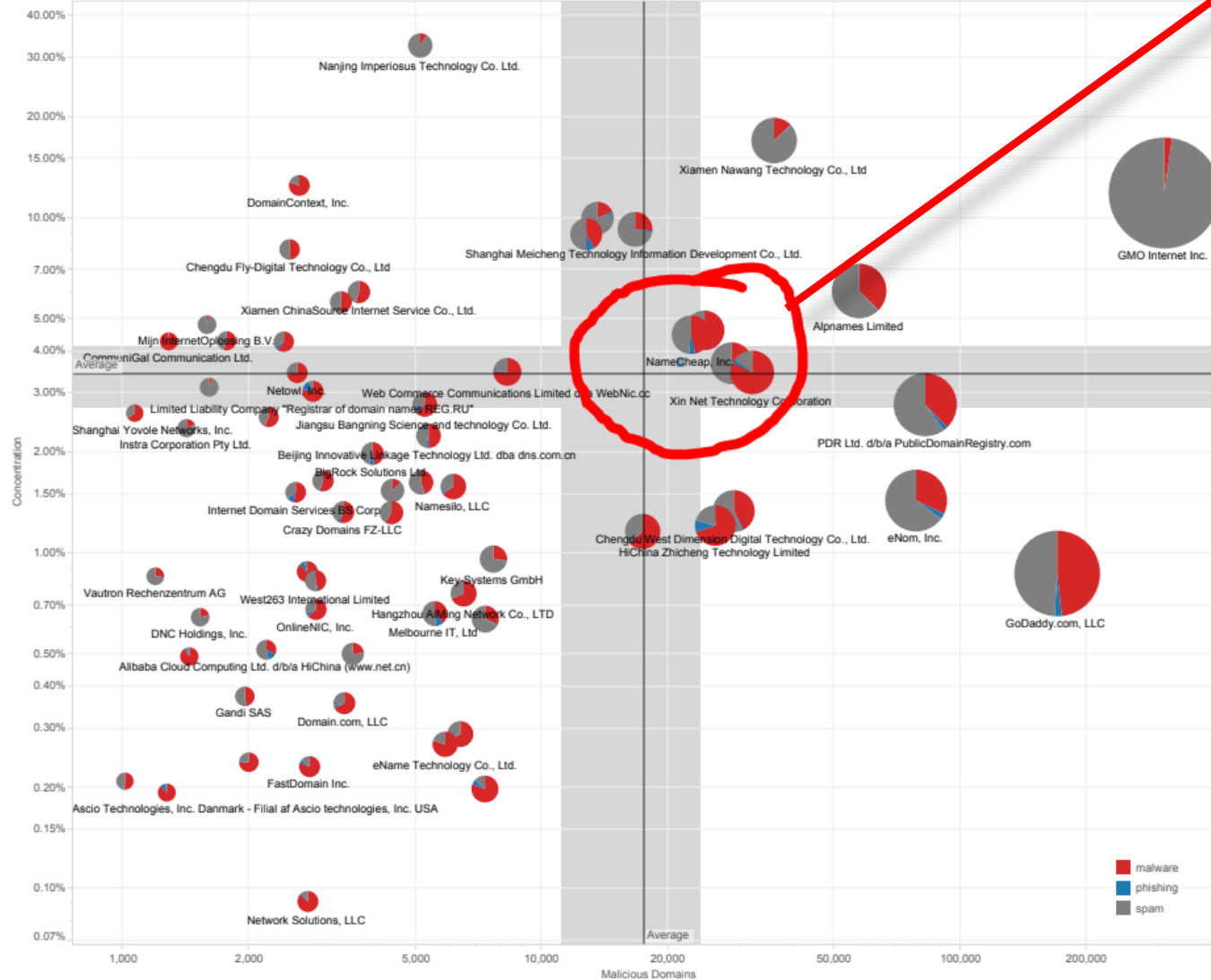
Observing the attack and the IP/Domains associated and with the initial help of the excellent job of Domaintools, we were able to cross-correlate two main elements:

- Registrar
- Hosting Provider



Registrars and Hosting providers Analysis

Malicious Domains by Registrar (Volume vs Concentration)



Considering the high usage of Namecheap for malicious purpose we can assume that this tendency is based on multiple factors: starting from the high volume of registered domain and arriving to the usage of services like Whoisguard and their «peculiar resistance» to collaborate unless intervention of law enforcement as other registrar of same «kind»

Most abused domain registrars, Q2 2020

When setting up a botnet C&C infrastructure, threat actors need to decide who they are going to register their domain with. Registrars can't easily detect fraudulent sign-ups; however, domains used for botnet C&Cs don't tend to have a long lifespan with well-run registrars.

Namecheap The US-based domain registrar Namecheap has been in the #1 spot for a significant length of time.

Enom Entering the Top 20 at #2, Enom had 419 botnet C&Cs operating on domains registered to it in Q2.

Highest climbers NameSilo had a 90% increase in the number of botnet C&Cs operating on domains registered through them in Q2, taking them to #3 on the Top 20 List. However, with an even more considerable increase of 202%, was Alibaba, moving up #11 in Q1 to #4 in Q2.

Most abused domain registrars - number of domains

Rank	Q2	% Change	Registrar	Country
#1	763	22%	Namecheap	United States
#2	419	New entry	Enom	United States
#3	304	90%	NameSilo	United States
#4	299	202%	Alibaba	China
#5	276	-10%	PDR	India
#6	275	-1%	WebNic.cc	Singapore
#7	263	-35%	Key-Systems	Germany
#8	204	49%	Eranet International	China
#9	178	-31%	west263.com	China
#10	161	New entry	OnlineNic	China
#11	137	-22%	Hosting Concepts	Netherlands
#12	124	-41%	RegRU	Russia
#13	95	New entry	Bizcn	China
#14	87	43%	Tucows	United States
#15	84	20%	55hl.com	China
#16	84	New entry	Meagazone	Korea
#17	80	45%	CentralNic	United Kingdom
#18	71	New entry	OVH	France
#19	55	-44%	NameBright/DropCatch	United States
#20	49	48%	Xin Net	China

Registrars and Hosting providers Analysis

Let's extend a bit our vision of the topic, by looking to Namecheap history...

On March 5, 2020, Facebook openly accused Namecheap and its Whoisguard proxy service, which manages the privacy of registrants, of allowing users to register domains that fool people into believing they are legitimate Facebook app domains¹.

Facebook

Protecting People from Domain Name Fraud

March 5, 2020
By Christen Dubois, Director and Associate General Counsel, IP Litigation

This week we filed a lawsuit in Arizona against Namecheap, a domain name registrar, as well as its proxy service, Whoisguard, for registering domain names that aim to deceive people by pretending to be affiliated with Facebook apps. These domain names can trick people into believing they are legitimate and are often used for phishing, fraud and scams.

Namecheap reaction²

According to Namecheap CEO Richard Kirkendall, "Where there is no clear evidence of abuse, or when it is purely a trademark claim, Namecheap will direct complainants, such as Facebook, to follow industry-standard protocol. Outside of said protocol, a legal court order is always required to provide private user information."

¹ <https://about.fb.com/news/2020/03/domain-name-lawsuit/>

² <https://uk.pcmag.com/social-networking/125155/facebook-sues-namecheap-over-domain-names-that-deceive>

Registrars and Hosting providers Analysis

«Another one bites the dust»

Domain: coronavirusmedicalkit[.]com

Another feud resolved with a federal judge ordering takedown:



Los Angeles-based Namecheap Inc. made the pledge after a federal judge in Texas ordered the takedown of a website the U.S. Department of Justice accused of stealing credit card information while offering fake coronavirus vaccine kits. The website allegedly offered what it claimed were World Health Organization vaccine kits in exchange for a \$4.95 “shipping charge.”

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

JOHN DOE, a/k/a
“coronavirusmedicalkit.com,”

Defendant.

Case No. A-20-CV-306

**] TEMPORARY RESTRAINING ORDER AND ORDER TO
SHOW CAUSE WHY A PRELIMINARY INJUNCTION SHOULD NOT ISSUE**

This matter comes before the Court on the United States’ Motion for a Temporary Restraining Order and Order to Show Cause Why a Preliminary Injunction Should Not Issue (the “Motion”). Upon consideration of the Motion pursuant to 18 U.S.C. § 1345, the Complaint for Temporary Restraining Order and Preliminary and Permanent Injunctions (the “Complaint”), and the Declaration of Supervisory Special Agent Jordan T. Loyd, the Court finds that:

1. This Court has jurisdiction over the subject matter of this case, there is good cause to believe that it will have jurisdiction over all the parties hereto, and venue in this district is proper.
2. There is probable cause to believe that Defendant Doe is violating and, unless enjoined, will continue to violate 18 U.S.C. § 1343.
3. The domain name “coronavirusmedicalkit.com,” which is registered by **NameCheap, Inc.**, 4600 East Washington Street Suite 305. Phoenix, AZ 85034, is being used as an instrumentality of Defendant’s crimes.

<https://abcnews.go.com/Technology/wireStory/internet-firm-restricts-virus-themed-website-registrations-69825166>

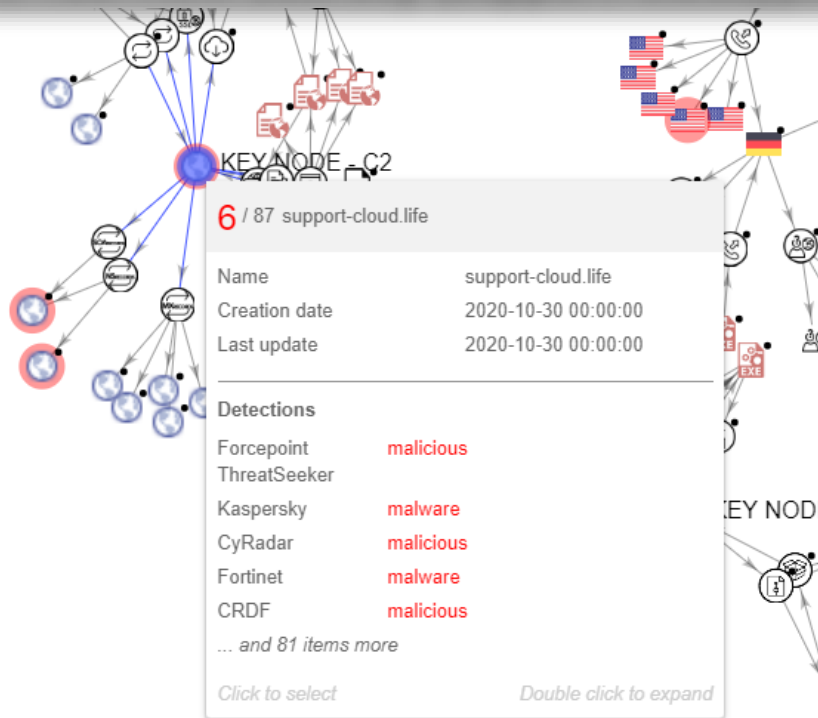
<https://www.justice.gov/opa/press-release/file/1260121/download/>

Registrars and Hosting providers Analysis

From our perspective, it is easy to see how direct the connection from the registrar to the attackers is when speak about Namecheap.

There are almost immediate matches, especially when we look to group potentially involved in the Sunburst/Solorigate campaign.

APT28: New Zebrocy (support-cloud[.]life)



Whois Record for Support-Cloud.life

Domain Profile	
Proximity Score	100
Email	abuse@namecheap.com is associated with ~14,136,478 domains
Registrar	NameCheap, Inc. IANA ID: 1068 URL: https://www.namecheap.com/ Whois Server: whois.namecheap.com abuse@namecheap.com (p) 16613102107

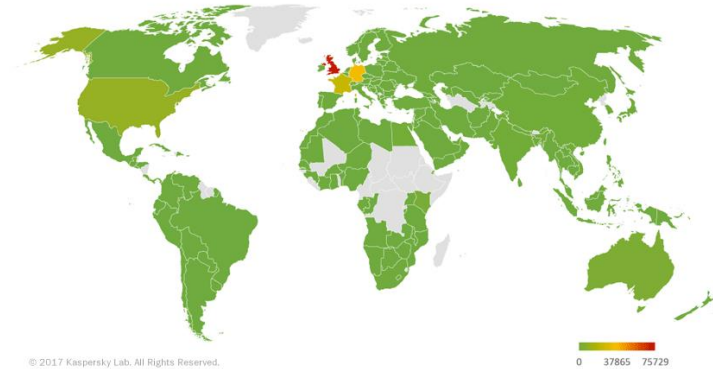
Registrars and Hosting providers Analysis

Another example related to a well-known malware like Dridex can be highlighted by an Infoblox report:

All the emails we observed were delivered by SMTP mail servers geolocated in Russia and configured to IP addresses in several classless inter-domain routing (CIDR) blocks.

The email senders were tied to accounts that used fraud domains with .club, .host, .site, and .xyz TLDs. The threat actor(s) selected several domain names and registered each one to all 4 TLDs. For example: domain[.]club, domain[.]host, domain[.]site, and domain[.]xyz.

All of the sender account domains were registered with Namecheap on 13 June. It is possible the threat actor(s) took advantage of Namecheap's recent domain registration sale to bulk configure the email bots.



The screenshot shows a threat intelligence interface. On the left, there's a sidebar with 'Basic Properties' and 'Relations'. The main area displays a graph with a node labeled '54 / 72' and a file details panel for a Win32 EXE file. The file name is 'MsRdpWebAccess.dll' and its size is 146.75 KB. It was first seen on 2017-02-16 and last seen on 2018-01-22. The interface also shows various detection engines and their results, such as 'Trojan.Inject12Lo7CVGOJs' and 'Trojan.Trojan.dab'.

We have seen how even sophisticated actors are attracted to this type of registrar and one of the reasons is plausibly the guarantee of privacy.

A tortuous speech with many facets that we leave with pleasure to the various disputes and law firms.

However, given the situation we looked to bind ATP-type actors or cybercriminals, with Registrants and we walked this path in Sunburst/Solorigate case with interesting results...

Russian APTs Adjacency

In order to continue the analysis starting from hypothesis that APT actors use Namecheap services we added a new cluster to include the Hosting Provider.

In addition, thanks to this operation we cross-correlated services like Namecheap and Solarigate Hosting Providers reported by the community.

This created an “adjacency”, a group of correlated information that permit new observations and inferences.

In fact, Among the various details we analyzed, we found a report from Area 1 report related to a phishing campaign on Burisma Holdings:

Since 2016, the GRU has consistently used an assembly line process to acquire and set up infrastructure for their phishing campaigns. Area 1 Security has correlated this campaign against Burisma Holdings with specific tactics, techniques, and procedures (TTPs) used exclusively by the GRU in phishing for credentials. Repeatedly, the GRU uses Itch, NameSilo, and NameCheap for domain registration; MivoCloud and M247 as Internet Service Providers; Yandex for MX record assignment; and a consistent pattern of lookalike domains.

Russian APTs Adjacency

After identifying the 7 domains registered on Namecheap and reported as linked with Sunburst/Solorigate, we carried out specific analysis of the relationship between these domains, the hosting providers and registrars.

databasegalore[.]com	14/12/2019	5.252.177.21	MivoCloud SRL	NAMECHEAP INC
freesonline[.]com	14/08/2014	54.193.127.66	Amazon Technologies Inc.	NAMECHEAP INC
incomeupdate[.]com	02/10/2016	5.252.177.25	MivoCloud SRL	NAMECHEAP, INC
mobilnweb[.]com	28/09/2019	172.97.71.162	Owned-Networks LLC	NAMECHEAP INC, NAMECHEAP, INC
seobundlekit[.]com	14/07/2019	3.16.81.254	Amazon Technologies Inc.	NAMECHEAP INC
swipeservice[.]com	03/09/2015	162.241.124.32	Unified Layer	NAMECHEAP INC, NAMECHEAP, INC
webcodez[.]com	12/08/2005	45.141.152.18	M247 Europe SRL	NAMECHEAP INC



The following domains, from the initial seven, are showing the characteristics described in the Area 1 report:



Domain	Host Provider	Registrar	Purpose
databasegalore[.]com	MivoCloud SRL	NAMECHEAP INC	Possible Beacon C2
incomeupdate[.]com	MivoCloud SRL	NAMECHEAP INC	Possible Beacon C2
webcodez[.]com	M247 Europe SRL	NAMECHEAP INC	Unknown

Operation Overtrap

ATTACKING TECHNIQUES

Cinobi

Another adjacency has been found with a campaign called “Operation Overtrap” with the banking trojan “Cinobi” targeting Japanese banking system.

The adjacency is highlighted by the fact that the `highdatabase[.]com` domain referred to the IP `139.99.115.204`, in the period of the attack, was resolving also `byte.inteleksys[.]com` and the hostname `sales.inteleksys[.]com`.

These domains are part of the Cinobi IOCs as reported by the TrendMicro and Niiconsulting.

Home » Operation Overtrap

Operation Overtrap Targets Japanese Online Banking Users Via Bottle Exploit Kit and Brand-New Cinobi Banking Trojan

Posted on: **March 11, 2020** at 6:00 am Posted in: **Malware** Author: **Trend Micro**



We recently discovered a new campaign that we dubbed “Operation Overtrap” for the numerous ways it can infect or trap victims with its payload. The campaign mainly targets online users of various Japanese banks by stealing their banking credentials using a three-pronged attack. Based on our telemetry, Operation Overtrap has been active since April 2019 and has been solely targeting online banking users located in Japan.

[READ MORE](#)

Threat Actors behind Operation Overtrap, found using Bottle Exploit Kit and Cinobi Banking Trojan for targeting customers of Banking & Financial Institutions in Japan

Severity: High
Date: March 12, 2020

IP ADDRESSES

- 139.99.115.204

DOMAINS

- shop.inteleksys.com
- view.inteleksys.com
- priv.inteleksys.com
- sales.inteleksys.com
- xizr.inteleksys.com
- byte.inteleksys.com
- ciox.inteleksys.com
- 5frjkw2w3ww6dnv.onion
- 4w6yniamu6x7e3a.onion
- bank-japanpostpo.jp
- bank-japanpost.jp
- bank-japanpostst.jp
- jp-bank.jp
- japanpost.jp
- ts3cardd.com
- security-amazon.jp
- safety-amazon.jp
- safeth-amazon.jp
- highdatabase.com
- agroaida.net
- ahoeab.org

REMIEDIATION

1. Immediately apply Security Patches for Microsoft vulnerabilities CVE-2020-0796, CVE-2020-0872, CVE-2020-0684, CVE-2020-0852, CVE-2020-0768, CVE-2020-0788, CVE-2020-0824, CVE-2020-0834, CVE-2020-0847, CVE-2020-0877, & CVE-2020-0887 on Windows Workstation and Server.
2. Immediately apply Security Patches for Microsoft vulnerabilities CVE-2020-0645, CVE-2020-0795, CVE-2020-0891, CVE-2020-0893, CVE-2020-0894, & CVE-2020-0903 on Microsoft IIS, SharePoint and Exchange Servers.
3. Strictly use least privilege accounts throughout the enterprise wide network.
4. Ensure to Disable SMB version 1 (SMBv1) on Windows server.
5. Strictly restrict inbound communication on Ports 135, 139, 445, and 3389, from external networks (internet).
6. Kindly restrict access on Ports 135, 139, 445, and 3389, for servers in production and access should only be granted when needed.
7. Ensure proper access control and email filtering are in place to protect Email Exchange Servers and Email Accounts.
8. Ensure PowerShell and Remote Desktop features are Disabled on nonadministrative systems in production environment.
9. Ensure internet facing devices, applications and services are using strong & complex passwords.
10. Closely monitor for any covert TCP/IP communications, and any suspicious activities, via SIEM solution.
11. File Integrity Monitoring for web application is strongly recommended.
12. Ensure IPS signatures related to above mentioned CVE IDs are put in prevent mode.
13. Strictly follow Zero-Trust strategy in Cyber Security Operations.
14. Kindly Block IPs and Domains on the perimeter security devices.
15. Kindly Block Hashes, that are not detected by your Antivirus Program or not known to your Antivirus Vendor.





Niiconsulting report of March 2020 about Operation Overtrap highlighting the presence of the `highdatabase.com` domain and the IP indicated as Solarigate's IOC

Cinobi adjacency

We have a further indication from AlienVault with respect to the indication of the IP to which is added an information that we are going to verify, namely the Country:

OTX details about 139.99.115.204

Passive DNS

STATUS ▾	HOSTNAME	QUERY TYPE	ADDRESS	FIRST SEEN	LAST SEEN	ASN	COUNTRY
▲ Suspicious	highdatabase.com	A	139.99.115.204	2020-12-14 08:24	2020-12-23 10:08	AS16276 OVH SAS	 Singapore
▲ Suspicious	byte.inteleksys.com	A	139.99.115.204	2020-03-11 06:46	2020-03-24 06:49	AS16276 OVH SAS	 Singapore
▲ Suspicious	play.mine-smp.me	A	139.99.115.204	2019-10-07 06:37	2019-10-07 06:37	AS16276 OVH SAS	 Singapore
▲ Suspicious	sales.inteleksys.com	A	139.99.115.204	2019-09-13 08:57	2019-10-12 02:28	AS16276 OVH SAS	 Singapore

Domaintools Hosting history highdatabase[.]com

Lookup the Hosting History of a Domain

highdatabase.com



IP Address History

Event Date	Action	Pre-Action IP	Post-Action IP
2019-03-08	New	-none-	52.58.78.16
2019-03-08	Not Resolvable	52.58.78.16	-none-
2019-03-20	New	-none-	91.195.240.126
2019-03-25	Change	91.195.240.126	52.58.78.16
2019-12-27	Change	52.58.78.16	139.99.115.204
2020-12-24	Change	139.99.115.204	85.17.31.82
2021-01-12	Change	85.17.31.82	5.79.71.205

The machine hosting the domains is an OVH VPS based in Singapore and, considering the extent of the resolution of the domains to it, we believe it possible that the same actor has access to this system to direct the two campaigns.

IP Information for 139.99.115.204

— Quick Stats

IP Location	 Singapore Singapore Ovh Singapore Pte. Ltd
ASN	 AS16276 OVH, FR (registered Feb 15, 2001)
Resolve Host	vps61.bachathost.ovh
Whois Server	whois.arin.net
IP Address	139.99.115.204

Cinobi adjacency

We tried to verify possible intersections between the various TTPs used in the two campaigns.

From the TrendMicro report about Cinobi, we noticed the network IOCs related to C2s published in Onion. This is interesting to narrow the circle of groups of attackers who, in the past, have used Onion for C2 or who in general use Tor in their attacks.



Domain	Description
shop[.]inteleksys[.]com	Bottle exploit kit domain
view[.]inteleksys[.]com	
priv[.]inteleksys[.]com	
sales[.]inteleksys[.]com	
xizr[.]inteleksys[.]com	
byte[.]inteleksys[.]com	
cionx[.]inteleksys[.]com	Cinobi V1 C&C domain
5frjkw2w3wv6dnv[.]onion	Cinobi V2 C&C Tor domain
4w6ylniamu6x7e3a[.]onion	
bank-japanpostpo[.]jpp	Phishing domain delivering Cinobi V1
bank-japanpost[.]com	
bank-japanposst[.]jpp	

Procedure Examples

Name	Description
APT29	A backdoor used by APT29 created a Tor hidden service to forward traffic from the Tor client to local ports 3389 (RDP), 139 (Netbios), and 445 (SMB) enabling full remote access from outside the network. ^[2]
Attor	Attor has used Tor for C2 communication. ^[3]
Dok	Dok downloads and installs Tor via homebrew. ^[4]
FIN4	FIN4 has used Tor to log in to victims' email accounts. ^[5]
GreyEnergy	GreyEnergy has used Tor relays for Command and Control servers. ^[6]
Inception	Inception used chains of compromised routers to proxy C2 communications between them and cloud service providers. ^[7]
Keydnab	Keydnab uses a copy of tor2web proxy for HTTPS communications. ^[8]
MacSpy	MacSpy uses Tor for command and control. ^[9]
StrongPity	StrongPity can use multiple layers of proxy servers to hide terminal nodes in its infrastructure. ^[9]
Tor	Traffic traversing the Tor network will be forwarded to multiple nodes before exiting the Tor network and continuing on to its intended destination. ^[10]
Ursnif	Ursnif has used Tor for C2. ^{[11][12]}
WannaCry	WannaCry uses Tor for command and control traffic. ^[13]

As we can notice, Russian threat actors are using TOR/Onion in different flavors, but not many non-Russian actors are using such techniques... This is gold when we try to “decode” the actors behind Sunburst as it seems the odds are pointing to East Europe, more than any other direction...

Raindrop & Cobaltstrike

REGISTRANTS

Raindrop & CobaltStrike

While we enriched this item with direct observation from our IR Team, we started the process from Symantec report related to Raindrop and its IOCs.

TEARDROP	
SHA256	b820e8a2057112d0ed73bd7995201dbed79a79e13c79d4bdad81a22f12387e07
URLs	https://infinitysoftwares(.)com/files/information_055.pdf https://infinitysoftwares(.)com/wp-admin/new_file.php
POST FORM	name="uploaded_1";filename="33139.pdf" Content-Type: text/plain
RAINDROP	
SHA256	be9dbbec6937dfe0a652c0603d4972ba354e83c06b8397d6555fd1847da36725
URLs	https://bigtopweb(.)com/files/page_306.pdf https://bigtopweb(.)com/wp-admin/admin-ajax.php
POST FORM	name="uploaded_1";filename="84921.pdf" Content-Type: text/plain

<https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-raindrop-malware>

Looking at the history related to a domain linked to Raindrop's C2, it was possible to identify the registrant's email address. As you can see from the figure, the registrant changes or is obscured by privacy before the attack.

2020-06-04	2020-06-18
1 Domain Name: bigtopweb.com	1 Domain Name: bigtopweb.com
2 Registry Domain ID: 2340071219_DOMAIN_COM-VRSN	2 Registry Domain ID: 2340071219_DOMAIN_COM-VRSN
3 Registrar WHOIS Server: whois.namesilo.com	3 Registrar WHOIS Server: whois.namesilo.com
4 Registrar URL: https://www.namesilo.com/	4 Registrar URL: https://www.namesilo.com/
5 Updated Date: 2020-05-22T07:00:00Z	5 Updated Date: 2020-06-17T07:00:00Z
6 Creation Date: 2018-12-04T07:00:00Z	6 Creation Date: 2018-12-04T07:00:00Z
7 Registrar Registration Expiration Date: 2020-12-04T07:00:00Z	7 Registrar Registration Expiration Date: 2021-12-04T07:00:00Z
8 Registrar: NameSilo, LLC	8 Registrar: NameSilo, LLC
9 Registrar IANA ID: 1479	9 Registrar IANA ID: 1479
10 Registrar Abuse Contact Email: abuse@namesilo.com	10 Registrar Abuse Contact Email: abuse@namesilo.com
11 Registrar Abuse Contact Phone: +1.4805240066	11 Registrar Abuse Contact Phone: +1.4805240066
12 Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited	12 Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
13 Registry Registrant ID:	13 Registry Registrant ID:
14 Registrant Name: Sergey Khromov	1 Registrant Name: Domain Administrator
15 Registrant Organization:	1 Registrant Organization: See PrivacyGuardian.org
16 Registrant Street: 16950-112 Collins Ave # 501	1 Registrant Street: 1928 E. Highland Ave. Ste F104 PMB 255
17 Registrant City: Sunny Isles Beach	1 Registrant City: Phoenix
18 Registrant State/Province: FL	1 Registrant State/Province: AZ
19 Registrant Postal Code: 33160	1 Registrant Postal Code: 85016
20 Registrant Country: US	2 Registrant Country: US
21 Registrant Phone: +1.2672571336	2 Registrant Phone: +1.3478717726
22 Registrant Phone Ext:	22 Registrant Phone Ext:
23 Registrant Fax:	23 Registrant Fax:
24 Registrant Fax Ext:	24 Registrant Fax Ext:
25 Registrant Email: sergey1313@gmail.com	25 Registrant Email: pw-

The update indicates a change in the domain and coincides with the IP change which will then be linked to the attack as IOC.

Raindrop & CobaltStrike

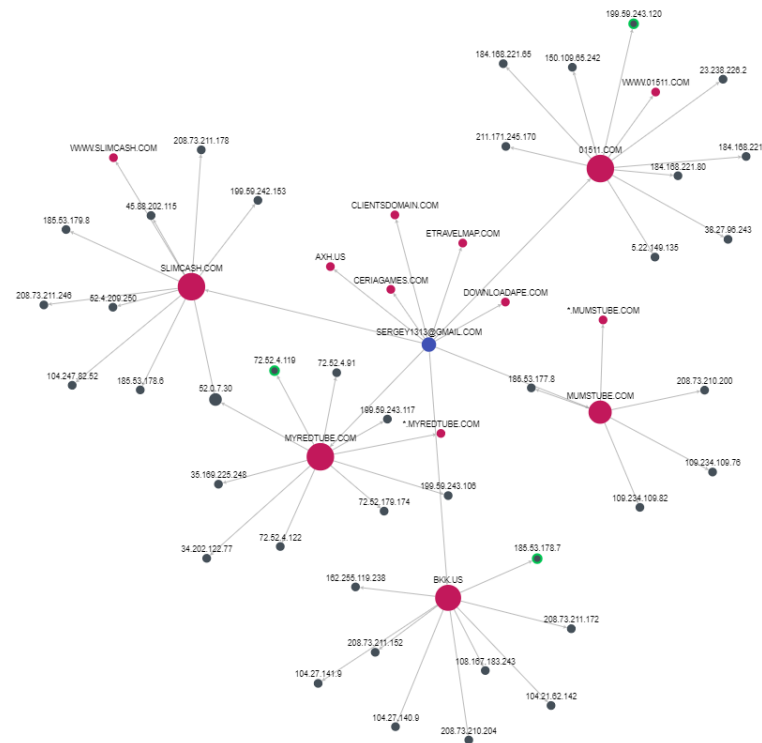
The figure shows the date of the IP change and the update in respect to the data described above

2019-02-15	Change	72.52.4.119	91.195.240.126
2020-06-18	Change	91.195.240.126	45.10.21.121

Through a verification carried out at the site:

<https://www.threatcrowd.org/email.php?email=sergey1313@gmail.com>

it is possible to check the relationships of the domains with the mail account.



EMAIL LOOKUP FOR SERGEY1313@GMAIL.COM

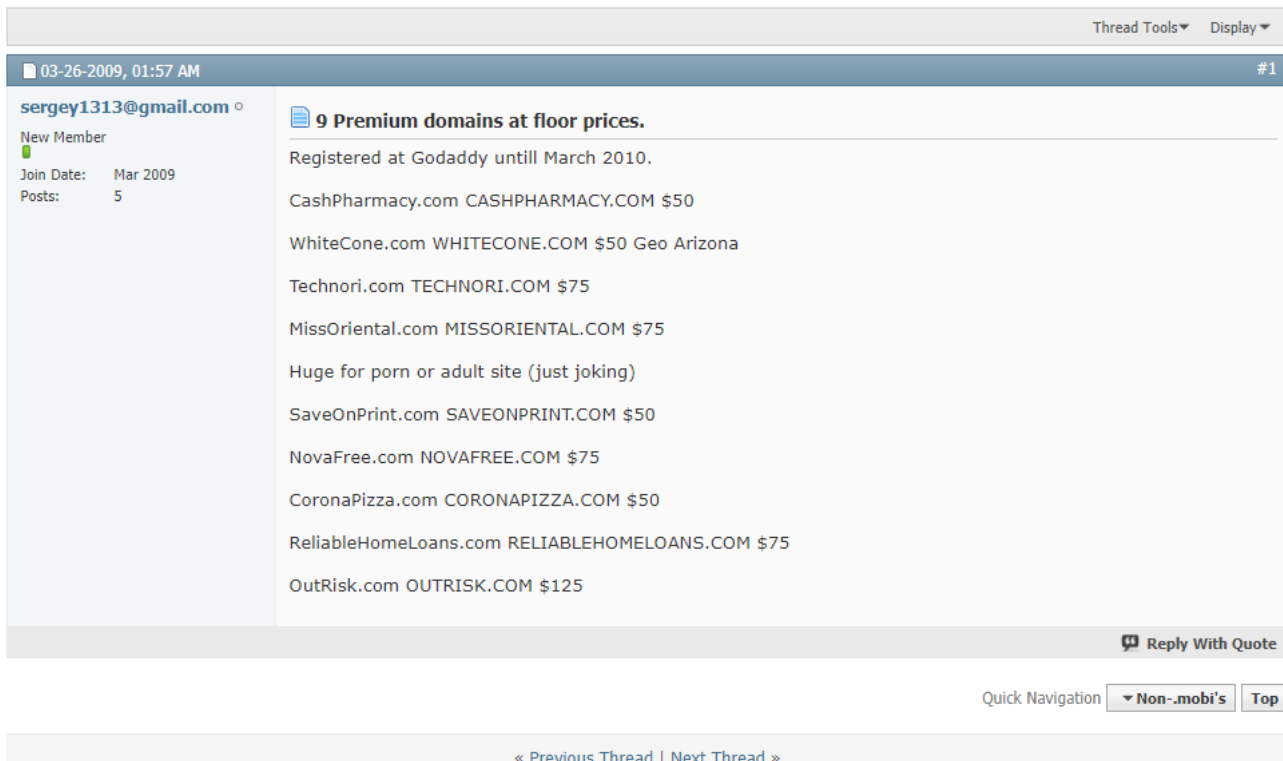
Welcome! Right click nodes and scroll the mouse to navigate the graph. ✕

REVERSE E-MAIL

Domain	Date
myredtube.com	2015-04-23
slimcash.com	2015-07-10
bkk.us	2015-08-14
munstube.com	2015-09-17
01511.com	2015-10-17
clientsdomain.com	2015-11-03
etravelmap.com	2015-12-23
axh.us	2015-12-25
downloadape.com	2015-12-25
cerigames.com	2016-01-21
lytst.com	2016-01-22
new.flip.so	2016-02-18
blackhatcourse.com	2016-03-11
solp.org	2016-03-22
abbotttravel.com	2016-05-21
120420.com	2016-05-26
webstish.com	2016-06-06

Looking for our friend Sergey...

Through a survey related to the same account we clarified the role of our friend Sergey.
He is a reseller of domains...



The screenshot shows a forum post from a user named sergey1313@gmail.com, who is a new member joined in March 2009. The post is titled "9 Premium domains at floor prices." and lists the following domains and their prices:

- Registered at Godaddy until March 2010.
- CashPharmacy.com CASHPHARMACY.COM \$50
- WhiteCone.com WHITECONE.COM \$50 Geo Arizona
- Technori.com TECHNORI.COM \$75
- MissOriental.com MISSORIENTAL.COM \$75
- Huge for porn or adult site (just joking)
- SaveOnPrint.com SAVEONPRINT.COM \$50
- NovaFree.com NOVAFREE.COM \$75
- CoronaPizza.com CORONAPIZZA.COM \$50
- ReliableHomeLoans.com RELIABLEHOMELOANS.COM \$75
- OutRisk.com OUTRISK.COM \$125

The post also includes a "Reply With Quote" button and a "Quick Navigation" section with buttons for "Non-.mobi's" and "Top".

<https://mobility.mobi/showthread.php?30080-9-Premium-domains-at-floor-prices&p=104204#post104204>

Our conclusions are confirmed by Threatconnect. This allows us to expand the perimeter related to the bigtopweb[.]com domain by including other domains with the same characteristics sold by the same individual during spring and summer 2020:

ThreatConnect Enrichment

Symantec's report identified several domains and other indicators associated with Raindrop, including bigtopweb.com (45.10.21.121). Like many of the previously identified SUNBURST domains, this domain was registered several years ago by a seemingly unrelated entity and then re-registered by the actor before it expired. With bigtopweb.com, the domain was registered in September 2018 and before it expired in late 2019, another actor -- sergey1313@gmail.com (likely a domain reseller) -- acquired the domain on 12/4/19. This actor held the domain until 6/17/2020 when the actor behind Raindrop most likely procured the domain and it was unparked and moved to NameSilo name servers.

The following domains were re-registered in spring/summer 2020 with similar characteristics, have SSL certificated consistent with other Raindrop / SUNBURST samples, and are hosted on dedicated servers like those previously identified:

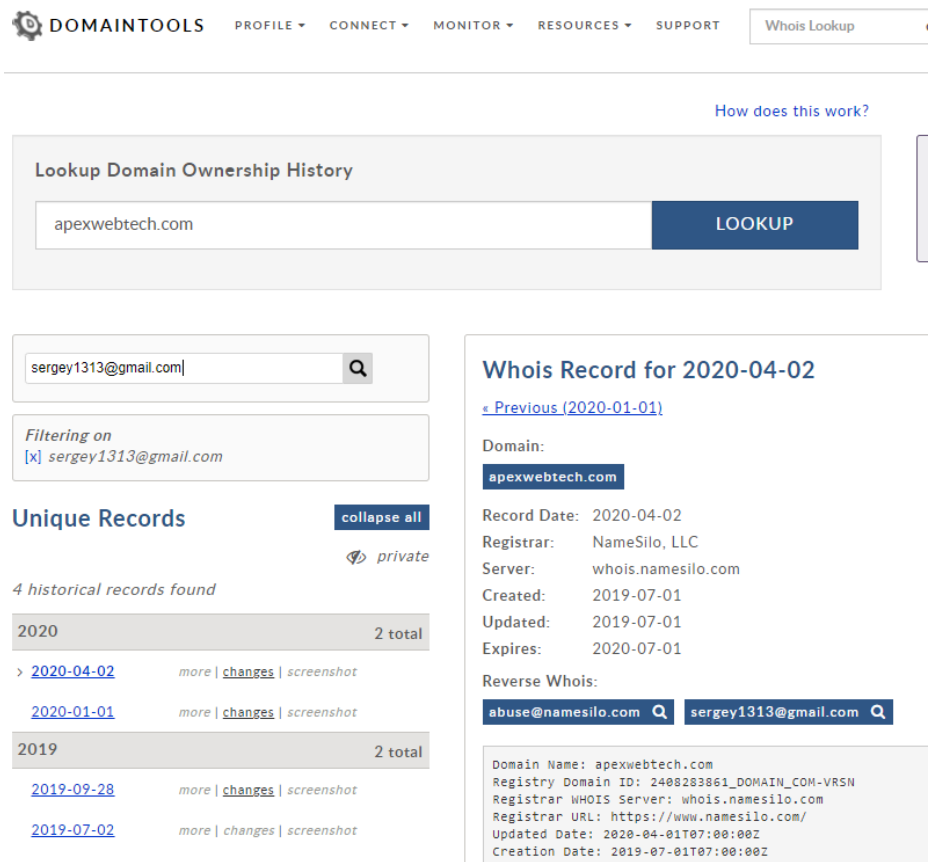
- apexwebtech.com (45.149.114.106)
- appsprovider.com (63.141.224.90)
- globesoftware.com (158.51.87.108)
- securitysystemnews.com (34.217.37.240)

At this time we don't have any additional information on the extent to which, if any, this infrastructure has been used maliciously.

<https://app.threatconnect.com/auth/incident/incident.xhtml?incident=4617777768#/tasks>

Peekaboo! Sergey...

We reviewed the results through Domaintools comparing our findings with Threatconnect.



DOMAINTOOLS PROFILE CONNECT MONITOR RESOURCES SUPPORT Whois Lookup

How does this work?

Lookup Domain Ownership History

apexwebtech.com LOOKUP

sergey1313@gmail.com

Filtering on [x] sergey1313@gmail.com

Unique Records collapse all private

4 historical records found

2020 2 total

> 2020-04-02 more | changes | screenshot

2020-01-01 more | changes | screenshot

2019 2 total

2019-09-28 more | changes | screenshot

2019-07-02 more | changes | screenshot

Whois Record for 2020-04-02

Previous (2020-01-01)

Domain: apexwebtech.com

Record Date: 2020-04-02

Registrar: NameSilo, LLC

Server: whois.namesilo.com

Created: 2019-07-01

Updated: 2019-07-01

Expires: 2020-07-01

Reverse Whois: abuse@namesilo.com sergey1313@gmail.com

Domain Name: apexwebtech.com
Registry Domain ID: 2408283861_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2020-04-01T07:00:00Z
Creation Date: 2019-07-01T07:00:00Z

With same procedure we was able to find other adjacencies with other domains in our Collection such as the one below:.

2020-02-14	2020-02-22
1 Domain Name: DATAZR.COM	1 Domain Name: DATAZR.COM
2 Registry Domain ID: 2429561560_DOMAIN_COM-VRSN	2 Registry Domain ID: 2429561560_DOMAIN_COM-VRSN
3 Registrar WHOIS Server: whois.epik.com	3 Registrar WHOIS Server: whois.epik.com
4 Registrar URL: http://www.epik.com	4 Registrar URL: http://www.epik.com
5 Updated Date: 2020-02-12T19:25:17Z	5 Updated Date: 2020-02-21T04:28:45Z
6 Creation Date: 2019-09-03T15:49:32Z	6 Creation Date: 2019-09-03T15:49:32Z
7 Registrar Registration Expiration Date: 2020-09-03T15:49:32Z	7 Registrar Registration Expiration Date: 2020-09-03T15:49:32Z
8 Registrar: Epik, Inc.	8 Registrar: Epik, Inc.
9 Registrar IANA ID: 617	9 Registrar IANA ID: 617
10 Registrar Abuse Contact Email: support@epik.com	10 Registrar Abuse Contact Email: support@epik.com
11 Registrar Abuse Contact Phone: +1.4253668810	11 Registrar Abuse Contact Phone: +1.4253668810
12 Reseller:	12 Reseller:
13 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited	13 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
14 Registry Registrant ID:	14 Registry Registrant ID:
15 Registrant Name: Anant Nag Chittamuru	15 Registrant Name: Privacy Administrator
16 Registrant Organization: n/a	16 Registrant Organization: Anonymize, Inc.
17 Registrant Street: No 51 Coconut Grove	17 Registrant Street: 704 228th Ave NE
18 Registrant City: Chennai	18 Registrant City: Sammamish
19 Registrant State/Province: 600042	19 Registrant State/Province: WA
20 Registrant Postal Code: 600042	20 Registrant Postal Code: 98074
21 Registrant Country: IN	21 Registrant Country: US
22 Registrant Phone: +91.9962278111	22 Registrant Phone: +1.4253668810
23 Registrant Phone Ext:	23 Registrant Phone Ext:
24 Registrant Fax:	24 Registrant Fax:
25 Registrant Fax Ext:	25 Registrant Fax Ext:
26 Registrant Email: anant.amazon@gmail.com	26 Registrant Email: datazr.com@anonymize.com
27 Registry Admin ID:	27 Registry Admin ID:
28 Admin Name: Anant Nag Chittamuru	28 Admin Name: Privacy Administrator
29 Admin Organization: n/a	29 Admin Organization: Anonymize, Inc.
30 Admin Street: No 51 Coconut Grove	30 Admin Street: 704 228th Ave NE
31 Admin City: Chennai	31 Admin City: Sammamish
32 Admin State/Province: 600042	32 Admin State/Province: WA

Conclusions

Conclusions

When we walk through a set of malware like this one, knowing the risk associated with their usage by the hand of an attacker, you can feel a bit “naked”.

The Sunburst/Solorigate attack leverages on a trusted and widely used application, implemented for pure monitoring. An application usually allowed to access Internet and allowed to poll systems in the network, to test network ports and to inherit, for its role, several benign firewall and intrusion detection rules.

We need to learn from this lesson, sophisticated attackers are always looking to opportunities like this one to get the chance to break into a network undetected and enjoy a relative advantage point of not raising suspicious alerts from their activities.

To avoid this risk, we need to develop a more coordinated mechanism enforcing additional controls upon applications such as Orion and, as we are far from ensuring that bulletproof providers are kept at bay, we need to push more attention to Threat Intel reports of such providers, as IR teams.

This is the only proactive way to reduce the window of exposure and the magnitude of breaches like this one, from the “victim” perspective.

The background is a vibrant red color with a grid of small, semi-transparent dots. Overlaid on this grid are several perspective lines that converge towards the center, creating a sense of depth and movement. The lines are also semi-transparent, allowing the grid to be seen through them.

RSA[®]