From RA Group to RA World: Evolution of a Ransomware Group

Executive Summary

The ransomware group RA Group, now known as RA World, showed a noticeable uptick in their activity since March 2024. About 37% of all posts on their dark web leak site have appeared since March, suggesting this is an emerging group to watch. This article describes the tactics, techniques and procedures (TTPs) used by RA World.

RA World uses a multi-extortion scheme, which usually includes exfiltrating sensitive data from its victims prior to encrypting it. The ransomware operators then use the exfiltrated data as leverage, threatening to post it on their website in case victims do not meet their ransom demands.

RA World notably experimented with a “cost per customer” calculation. Below victim entries, they posted comments such as, “This company isn’t willing to pay $0.5 per customer to protect their privacy.”

Analysis of the posts on their leak site shows that RA World mainly impacted organizations in the healthcare industry until recently. The group did not appear to have any particular qualms about attacking organizations in a sensitive sector such as healthcare. Midway through 2024, manufacturing became the sector most impacted by the group. It is possible that the shift came from a desire to attack organizations more likely to be able to pay higher ransoms. However, many ransomware groups are simply opportunistic, and it is also possible the change was incidental.

The U.S. is the country most affected by these attacks, followed by countries in Europe and Southeast Asia.

Palo Alto Networks customers are better protected against the ransomware used by RA World through the following products and services:

- Cortex XDR and XSIAM
- Cloud-Delivered Security Services for the Next-Generation Firewall such as Advanced WildFire and Advanced URL Filtering

The Cortex XDR anti-ransomware module includes out-of-the-box protections that prevent adverse behavior from the ransomware samples we tested, without the need for specific detection logic or signatures.

The Prisma Cloud Defender should be deployed on cloud-based Windows virtual machines for better protection against the ransomware used by the RA World. Cortex Xpanse is able to provide visibility that can prove valuable for proactive protection.

The Unit 42 Incident Response team can also be engaged to help with a compromise or to provide a proactive assessment to lower your risk.

Related Unit 42 Topics	**Ransomware**, **Extortion**

RA World Overview

Ever since Talos first described it in 2023, RA World has been steadily active. Out of the organizations it has publicly claimed to have breached, the largest number were in the manufacturing sector. Figure 1 below details the statistics of different sectors affected by the RA World. The data covers the period from mid-2023 to June 6, 2024.

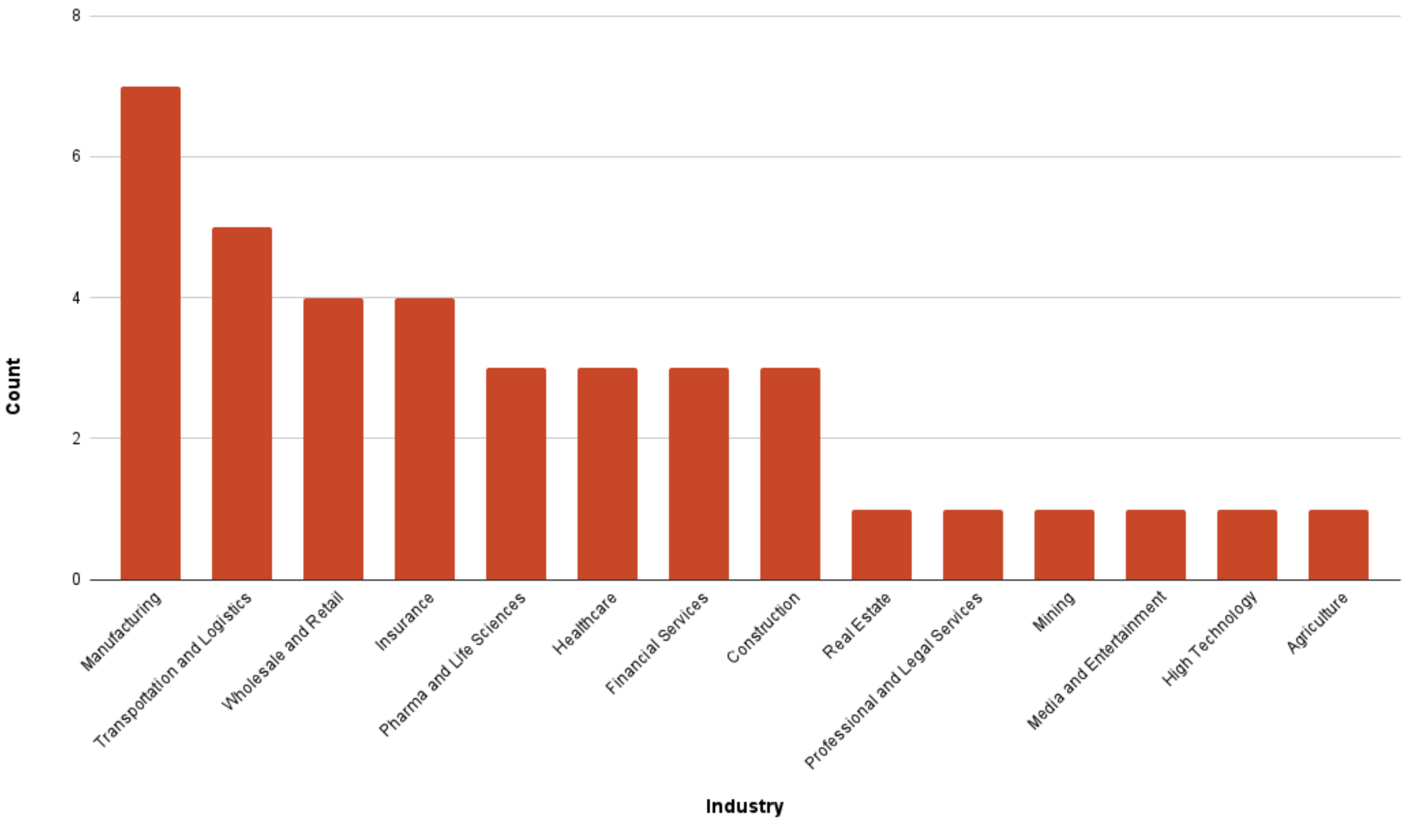
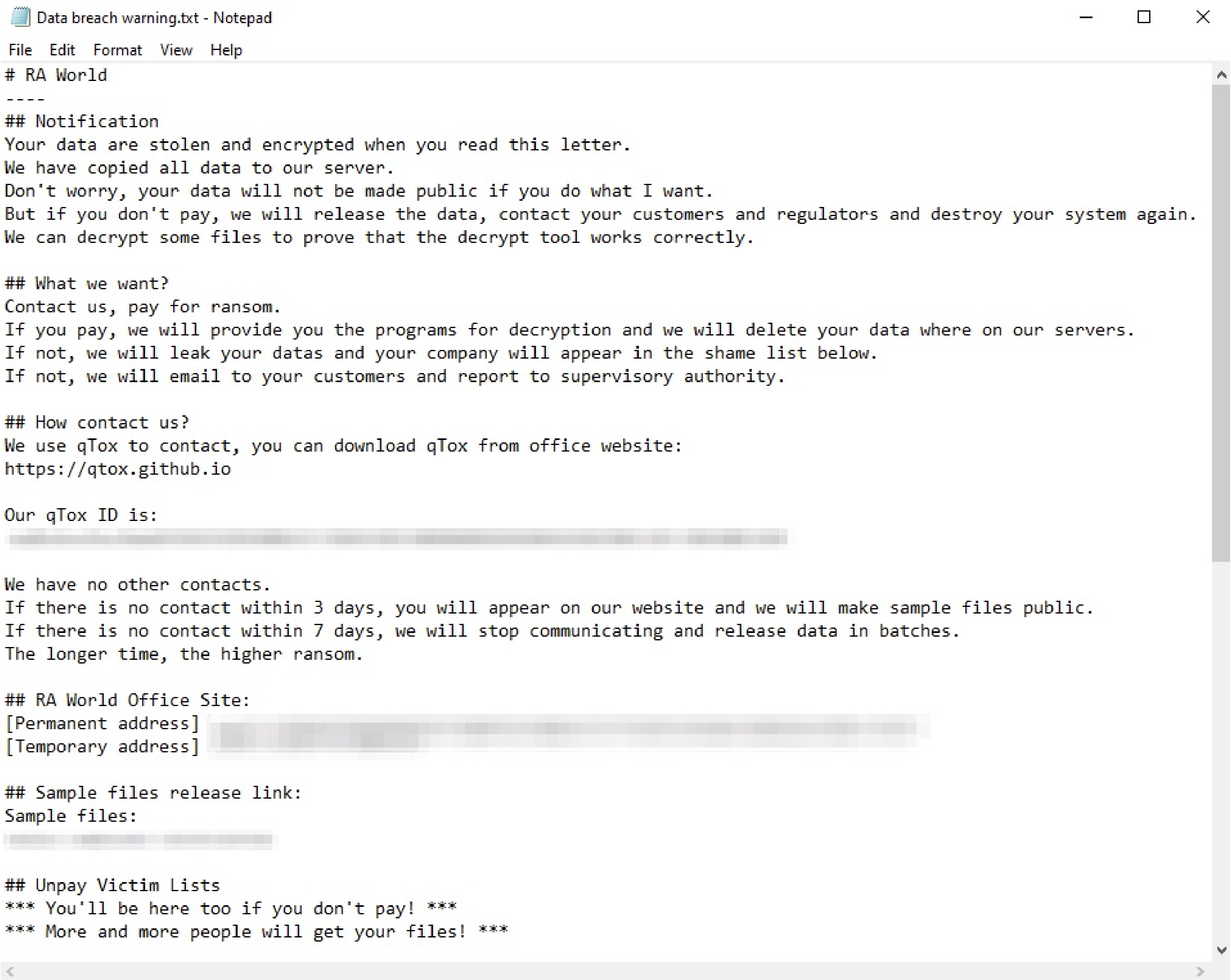


Figure 1. A bar chart showing the victims of the RA World group by sector, according to posts on the group’s dark web leak site.

According to analysis of leak site data, RA World impacts organizations based in the U.S. the most. The group has also impacted organizations in several countries in Europe, such as Germany and France. In Asia, organizations in Taiwan were impacted. In addition, Trend Micro reported that the group recently carried out a campaign affecting organizations in South America.

When RA World renamed its gang from RA Group, they also changed their encrypted file extensions to `.RAWLD`. In addition, they changed the title and content of their ransom note to include their new name, as shown in Figure 2 below.



```
# RA World
----
## Notification
Your data are stolen and encrypted when you read this letter.
We have copied all data to our server.
Don't worry, your data will not be made public if you do what I want.
But if you don't pay, we will release the data, contact your customers and regulators and destroy your system again.
We can decrypt some files to prove that the decrypt tool works correctly.

## What we want?
Contact us, pay for ransom.
If you pay, we will provide you the programs for decryption and we will delete your data where on our servers.
If not, we will leak your datas and your company will appear in the shame list below.
If not, we will email to your customers and report to supervisory authority.

## How contact us?
We use qTox to contact, you can download qTox from office website:
https://qtox.github.io

Our qTox ID is:
[redacted]

We have no other contacts.
If there is no contact within 3 days, you will appear on our website and we will make sample files public.
If there is no contact within 7 days, we will stop communicating and release data in batches.
The longer time, the higher ransom.

## RA World Office Site:
[Permanent address] [redacted]
[Temporary address]

## Sample files release link:
Sample files:
[redacted]

## Unpay Victim Lists
*** You'll be here too if you don't pay! ***
*** More and more people will get your files! ***
```

Figure 2. RA World's revamped ransom note.

Leak Site

RA World maintains a leak site, where the group uploads portions of the stolen data they exfiltrate from their victims to coerce ransom payments. Their website's design also looks upgraded compared to their old website's simple look that was shown in previous research in 2023. Figures 3 and 4 below show the two recent iterations of the leak site's main page.

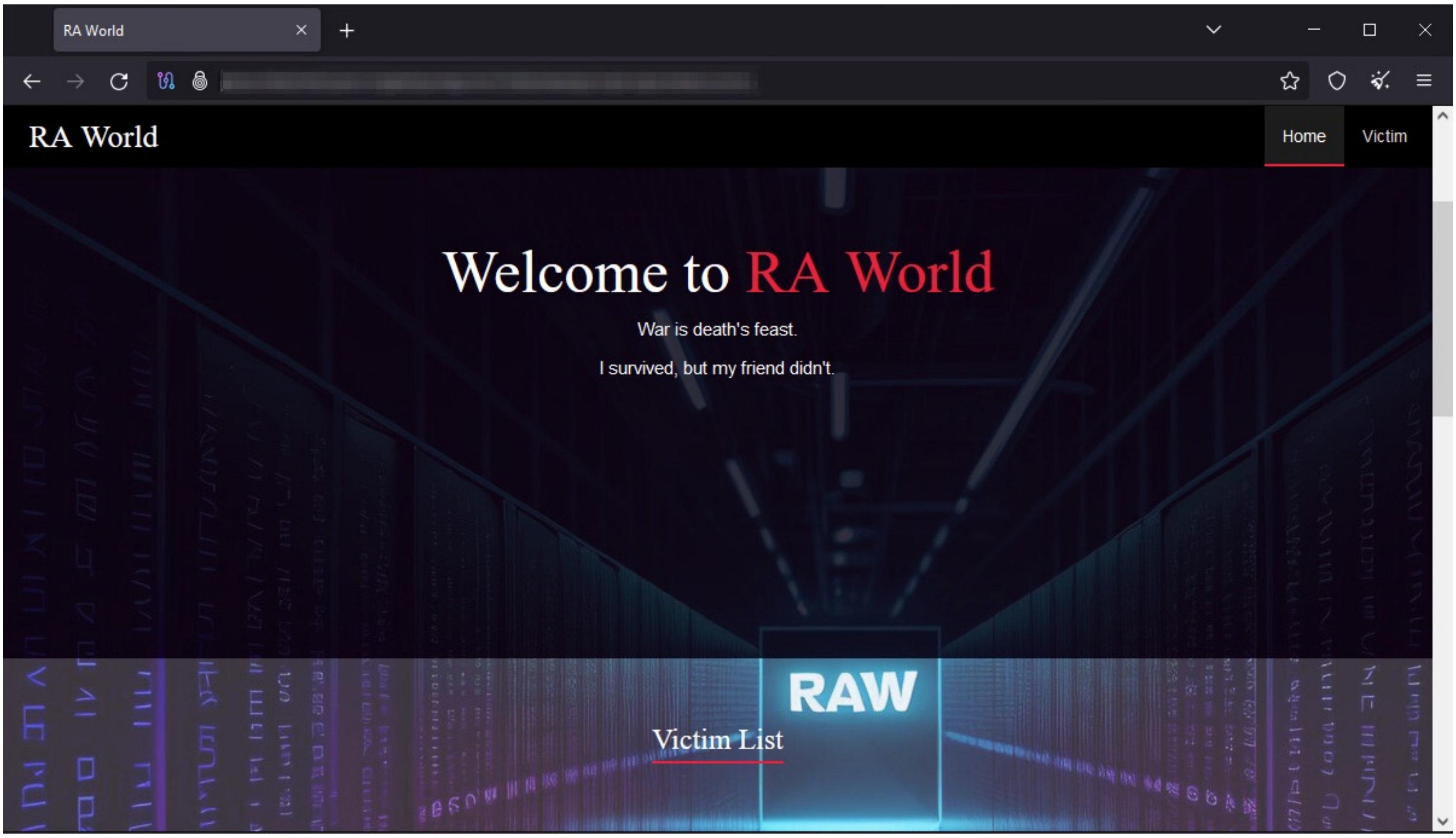
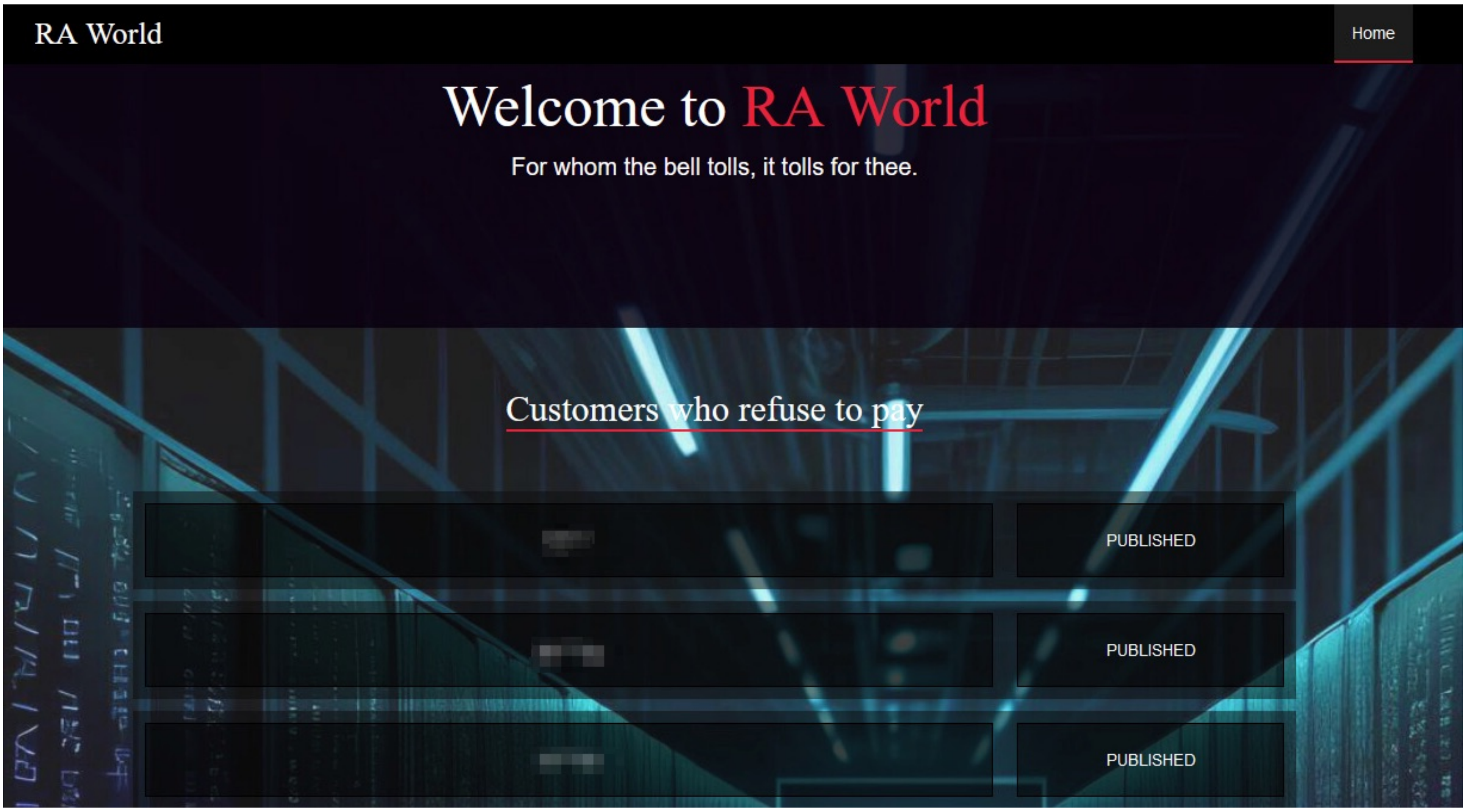


Figure 3. RA World’s leak site main page from early 2024.

In the website’s most recent version, they display a famous line from the work of English poet John Donne, “for whom the bell tolls, it tolls for thee” on the main page. Threat actors also use this line as the string for the mutex in their final payload, the Babuk ransomware.



RA World

Home

Welcome to RA World

For whom the bell tolls, it tolls for thee.

Customers who refuse to pay

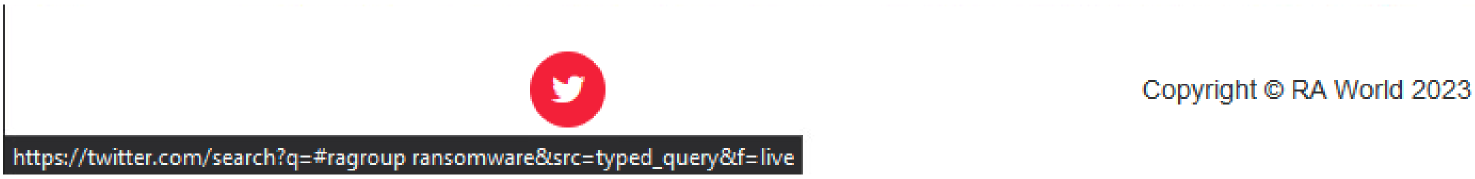
[redacted] PUBLISHED

[redacted] PUBLISHED

[redacted] PUBLISHED

Figure 4. RA World’s current leak site main page.

Figure 5 shows the bottom portion of the group’s main page, which contains a link to an X (formerly Twitter) search. The right-hand side of the screenshot claims a “copyright” for the site under their new RA World name, but as of this writing, the X search link still points to the older search term, `ragroup`.



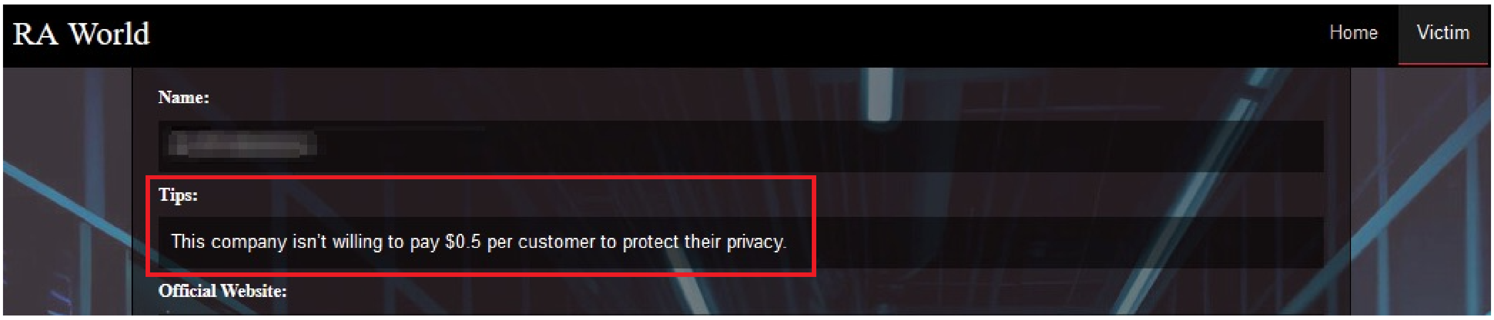
Copyright © RA World 2023

https://twitter.com/search?q=#ragroup ransomware&src=typed_query&f=live

Figure 5. RA World’s reference to a related X search at the bottom of their leak site.

X is considered a major platform for security vendors and researchers to share findings, so it would make sense for the threat actor to follow use of their name for publications about their activity.

Figure 6 shows a victim’s leak page from early 2024 where RA World attempted to publicly damage the victim’s reputation by stating what they allege is the real “cost per customer.” They arrive at this figure by taking the total requested ransom amount divided by the number of the victim’s customers, if the victim is a customer-facing company. They frame this figure in terms of what the victim is unwilling to pay to “protect their customers’ privacy.”



RA World

Name:

[redacted]

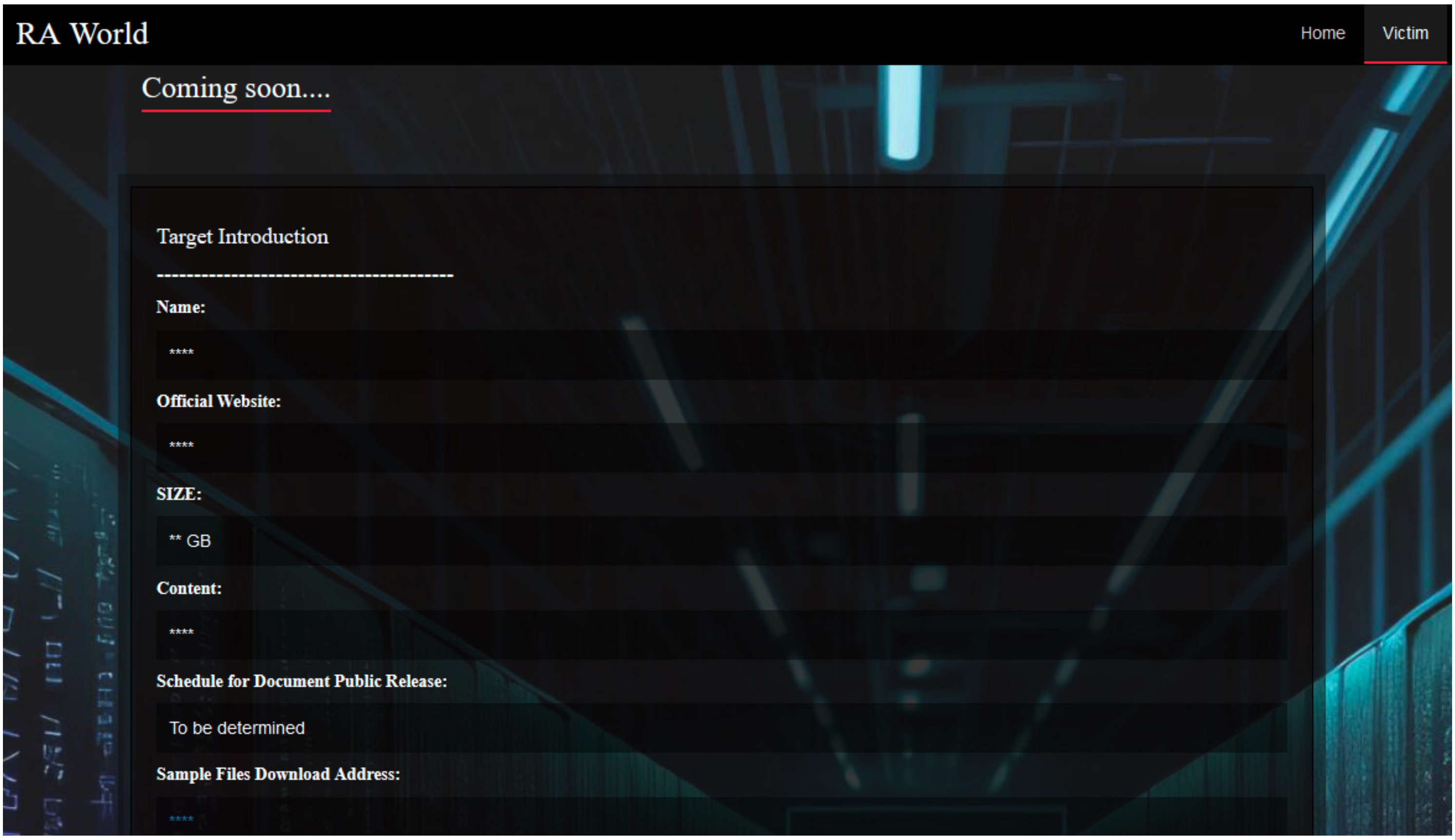
Tips:

This company isn't willing to pay $0.5 per customer to protect their privacy.

Official Website:

Figure 6. An example of a victim’s webpage on RA World’s leak site.

The threat actors updated the victim’s leak page in the leak site's recent version, as shown in Figure 7 below. They removed the “cost per customer” figure, but they added a “Coming soon….” section that displays new victims who will soon be listed. This section is most likely meant to include victims who were not willing to pay the ransom, and RA World is still in the process of uploading their exfiltrated data.



Coming soon....

Target Introduction

Name:

****

Official Website:

****

SIZE:

** GB

Content:

****

Schedule for Document Public Release:

To be determined

Sample Files Download Address:

****

Figure 7. An example of a victim's "coming soon" webpage on RA World's leak site's recent version.

Technical Analysis

We have mapped the attack stages using the MITRE ATT&CK framework to activities that are common to RA World.

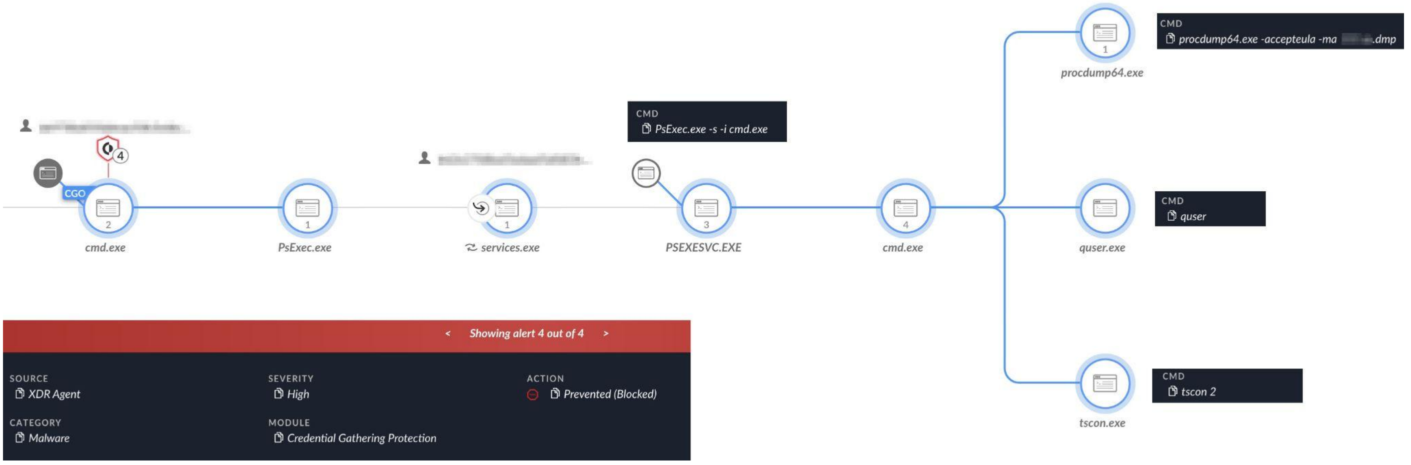
Initial Access

Based on our telemetry, RA World predominantly exploits misconfigured or vulnerable internet-facing servers. We have not observed instances of phishing attacks to gain initial access to the environment.

Credentials Dumping

We observed the threat actor attempting to use the PsExec utility to dump credentials by executing another SysInternals tool, ProcDump. They also attempted to run the `quser` and `tscon` commands to retrieve data about the current user and remote session.

Figure 8 below shows Cortex XDR prevented these attempts.



CMD
```
PsExec.exe -s -i cmd.exe
```

CMD
```
procdump64.exe -accepteula -ma [redacted].dmp
```

CMD
```
quser
```

CMD
```
tscon 2
```

< Showing alert 4 out of 4 >

SOURCE
XDR Agent

SEVERITY
High

ACTION
Prevented (Blocked)

CATEGORY
Malware

MODULE
Credential Gathering Protection

Figure 8. A prevented attempt of executing multiple commands as seen in Cortex XDR.

Lateral Movement

To move laterally in the compromised network and execute commands on remote endpoints, RA World used the popular Impacket tool. They executed remote commands to dump the SAM hive, copied the NTDS database and exported the system registry.

The threat actor then used the `makecab` utility to archive the databases and deleted the previously extracted database files from disk. Table 1 below shows the commands and their descriptions.

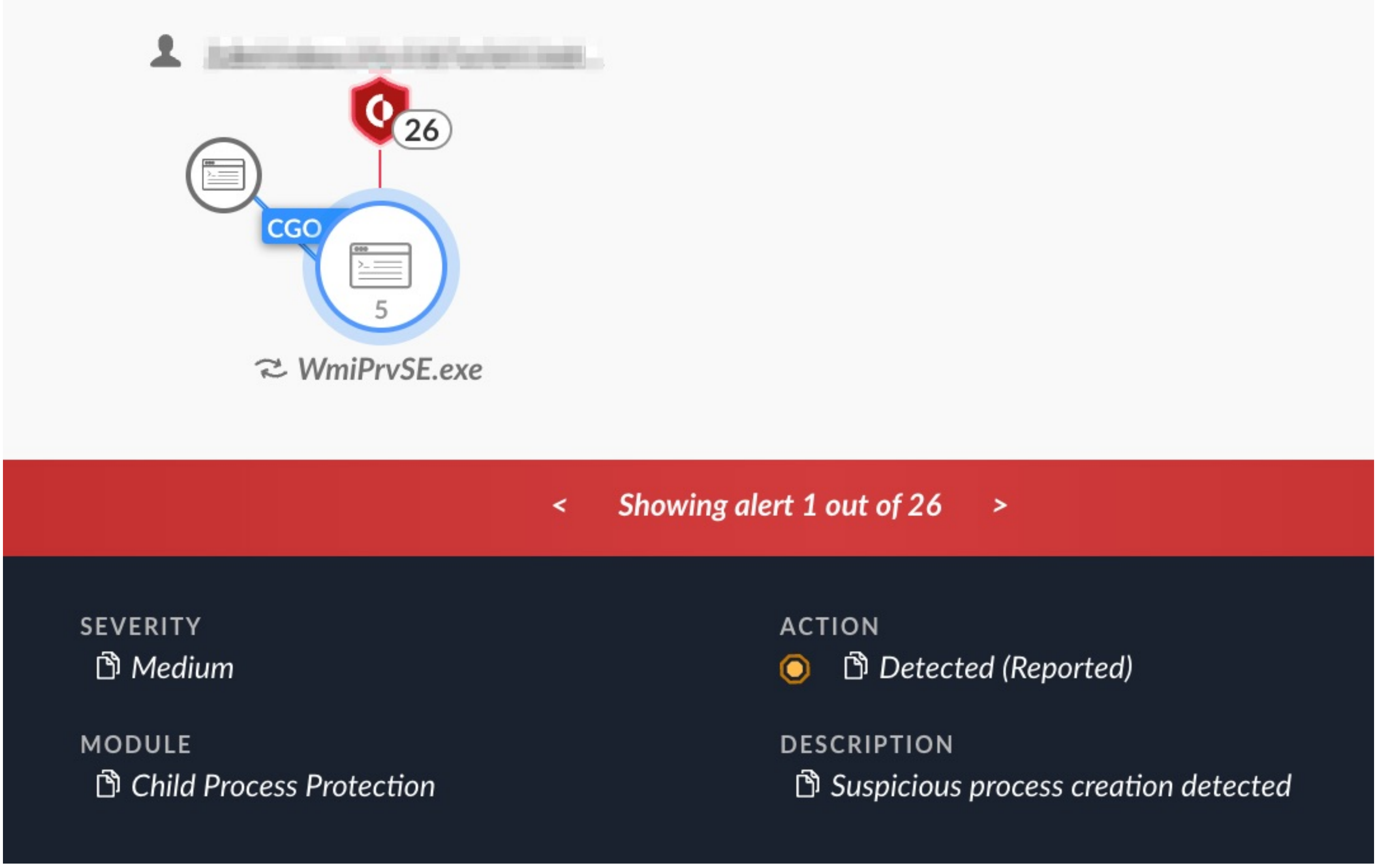
Command	Description

`cmd.exe /Q /c copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3\windows\NTDS\ntds.dit [redacted].dit 1> \\127.0.0.1\ADMIN$\__1706227818.9154336 2>&1`	Copying the NTDS database
`cmd.exe /Q /c copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3\Windows\System32\config\SAM [redacted].hiv 1> \\127.0.0.1\ADMIN$\__1706227818.9154336 2>&1`	Exporting the SAM hive
`cmd.exe /Q /c copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3\Windows\System32\config\SYSTEM [redacted].hiv 1> \\127.0.0.1\ADMIN$\__1706227818.9154336 2>&1`	Exporting the system's registry
`cmd.exe /Q /c makecab [redacted].dit [redacted].zip 1> \\127.0.0.1\ADMIN$\__1706227818.9154336 2>&1`	An example of archiving the NTDS database

Table 1. The RA World's lateral movement and credentials dumping commands and their respective descriptions.

The attackers executed the above commands under the Windows Management Instrument (WMI) Provider Host.

Figure 9 shows the alerts raised when Cortex XDR detected them.



SEVERITY
Medium

ACTION
Detected (Reported)

MODULE
Child Process Protection

DESCRIPTION
Suspicious process creation detected

Figure 9. An alert of malicious WMI activity as seen in Cortex XDR in detect mode.

Persistence and Impact: A Multi-Stage Ransom Infection Chain

Germán Fernández, a security researcher from Chile, tweeted about various artifacts found in a ransomware attack by RA World earlier this year. The artifacts he mentioned include various executable files and scripts.

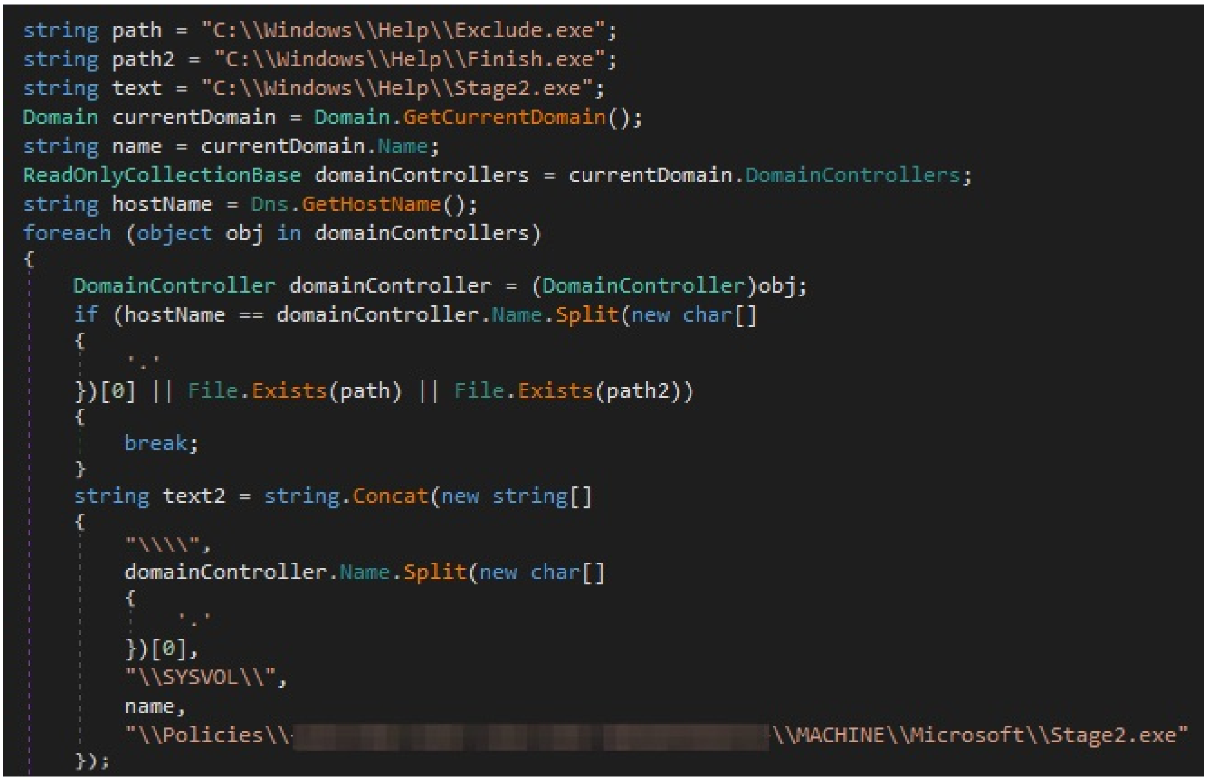
Trend Micro published the first public report of RA World's updated tool set in early March 2024. Their analysis of the files revealed several stages, each having its own role in the infection process prior to the delivery of the final ransomware payload.

Stage 1: Loader

The initial loader, also known as `Stage1.exe`, has two main roles:

- Perform a variety of checks including assessing the domain name and looking for a file called `Exclude.exe`. Judging by its name, this file could contain exclusions such as specific machines and file paths.
- Add `Stage2.exe` to the SYSVOL shared path and then execute it.

The loaders are usually small files with a maximum size of about 10 KB. Figure 10 below shows most of the loader’s code.



```
string path = "C:\\Windows\\Help\\Exclude.exe";
string path2 = "C:\\Windows\\Help\\Finish.exe";
string text = "C:\\Windows\\Help\\Stage2.exe";
Domain currentDomain = Domain.GetCurrentDomain();
string name = currentDomain.Name;
ReadOnlyCollectionBase domainControllers = currentDomain.DomainControllers;
string hostName = Dns.GetHostName();
foreach (object obj in domainControllers)
{
    DomainController domainController = (DomainController)obj;
    if (hostName == domainController.Name.Split(new char[]
    {
        '.'
    })[0] || File.Exists(path) || File.Exists(path2))
    {
        break;
    }
    string text2 = string.Concat(new string[]
    {
        "\\\\",
        domainController.Name.Split(new char[]
        {
            '.'
        })[0],
        "\\SYSVOL\\",
        name,
        "\\Policies\\[redacted]\\MACHINE\\Microsoft\\Stage2.exe"
    });
```

Figure 10. A code snippet from Stage1.exe showing its exclusion of files and information gathering about domain controllers.

Stage 2: Enable Safe Mode and Deliver Babuk

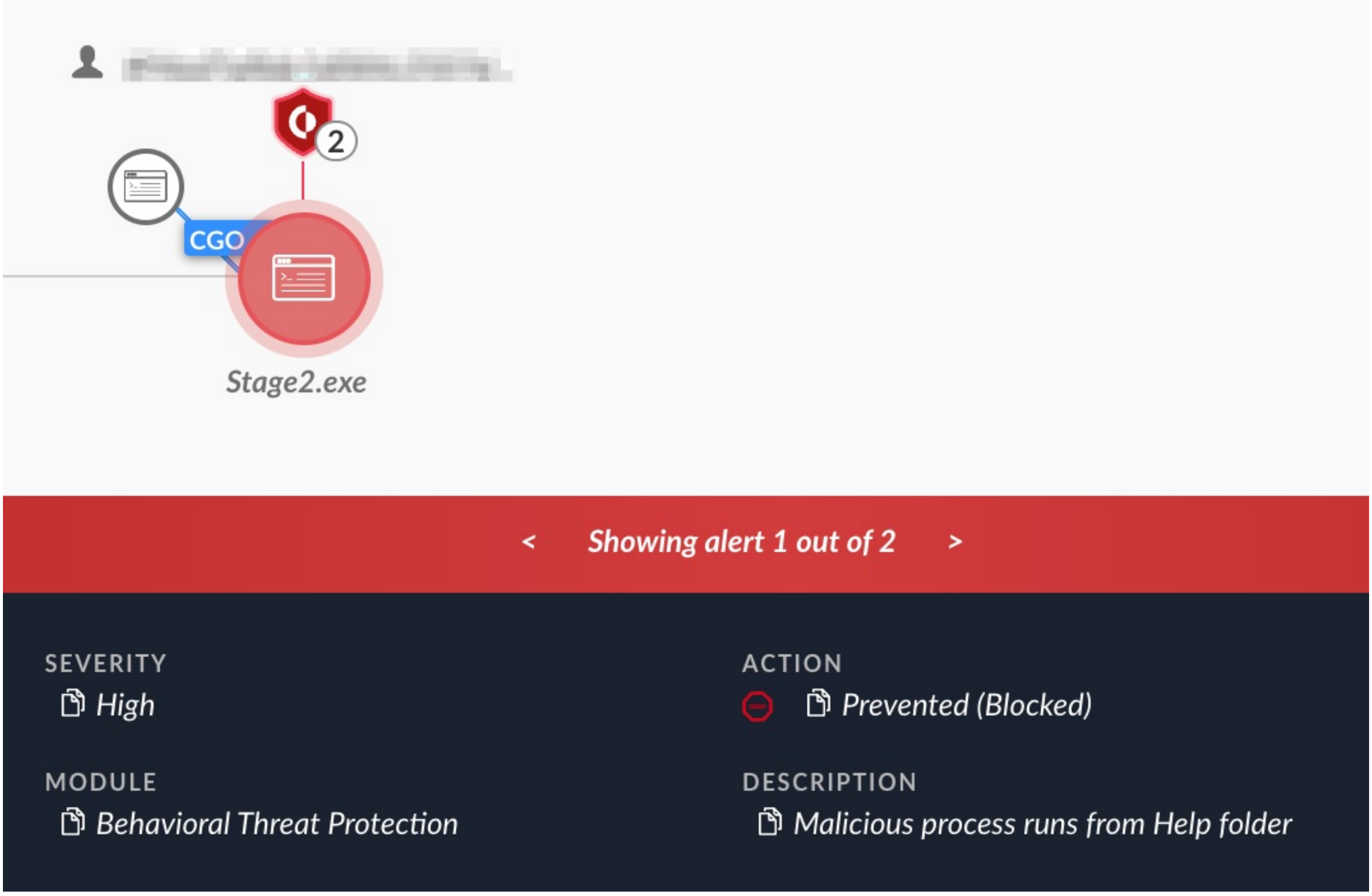
The next stage of the infection chain has two separate operation mechanisms that are dependent on whether or not the system is running in safe mode. `Stage3.exe` must be run in safe mode so it can evade detection by security solutions that, by default, won’t run in this mode. This file is the final ransomware payload, and a new Babuk variant.

If the system is operating in safe mode, the Babuk binary will be decrypted using Advanced Encryption Standard (AES) and then executed, followed by an attempt to disable safe boot. The AES key and initiation vector are generated based on the victim's local domain name, which the malware would previously have retrieved in `Stage1.exe`.

Otherwise, `Stage2.exe` will write itself as a service to the compromised machine, using the following command:

```
reg add
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\MSOfficeRunOncelsls" /t REG_SZ /d Service /f
```

Figure 11 shows the execution of `Stage2.exe` that Cortex XDR detected and prevented.



< Showing alert 1 out of 2 >

SEVERITY
High

ACTION
Prevented (Blocked)

MODULE
Behavioral Threat Protection

DESCRIPTION
Malicious process runs from Help folder

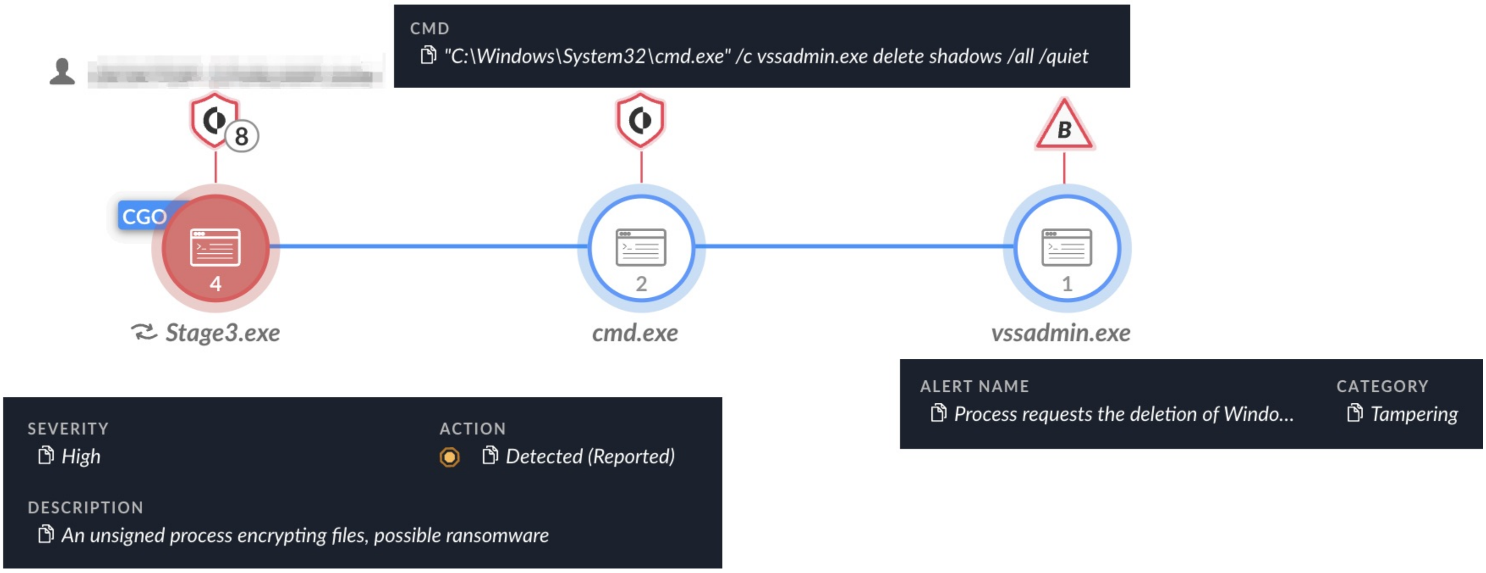
Figure 11. A description of a prevention alert.

Stage 3: New Variant of the Babuk Final Payload

Since its discovery in mid-2023, RA World has used a customized version of the Babuk ransomware, which had its source code leaked in 2021. In its recent activity, RA World has updated their Babuk-based payload with some relatively minor changes. Changes in this variant include:

- Changing the mutex name from `DoYouWantToHaveSexWithCuongDong` to `For whom the bell tolls, it tolls for thee`
- Changing the ransom note filename from `How To Restore Your Files.txt` to `Data breach warning.txt`
  - Modifying the note’s content accordingly
- Changing the encrypted file extension to `.RAWLD` from `.GAGUP`
- Stripping down the previous variant’s PDB path
- Creating the file `C:\Windows\Help\Finish.exe` to indicate the encryption process is finished
- Adding more filenames, paths, processes and service names to exclude during encryption

Figures 12 and 13 show Cortex XDR detecting and preventing the execution of RA World’s Babuk payload.



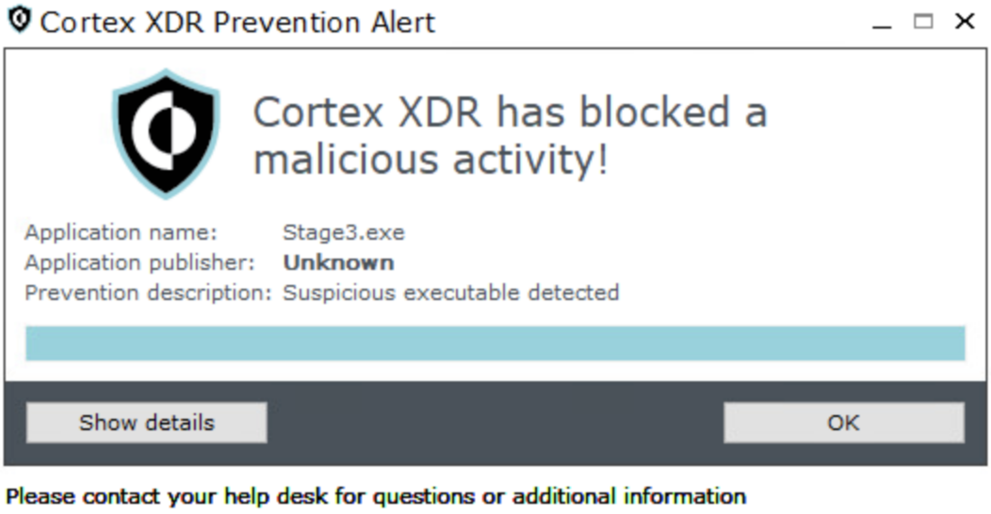
CMD
"C:\Windows\System32\cmd.exe" /c vssadmin.exe delete shadows /all /quiet

ALERT NAME: Process requests the deletion of Windo...
CATEGORY: Tampering

SEVERITY: High
ACTION: Detected (Reported)

DESCRIPTION: An unsigned process encrypting files, possible ransomware

Figure 12. Detection of the Babuk ransomware payload as seen in Cortex XDR in detect mode.



Cortex XDR Prevention Alert

Cortex XDR has blocked a malicious activity!

Application name: Stage3.exe
Application publisher: **Unknown**
Prevention description: Suspicious executable detected

Please contact your help desk for questions or additional information

Figure 13. A prevention alert of the Babuk ransomware payload as seen in Cortex XDR in prevent mode.

RA World's TTP Similarities With BRONZE STARLIGHT: A Possible, Yet Unverified, Connection

During our research, we identified some connections in the forensic data found in our telemetry that, with a low-confidence attribution level, tie RA World with BRONZE STARLIGHT (aka Emperor Dragonfly). BRONZE STARLIGHT is a Chinese threat group that deploys different ransomware payloads.

Several of the TTPs we found overlapped with TTPs used by BRONZE STARLIGHT, as discussed by Sygnia in 2022**.**

- **NPS tool use:** During our research, we found that the attackers were using NPS, an open-source tool created by a Chinese developer. The tool's latest release was back in 2021, and it's mainly used by Chinese threat actors. According to Sygnia, BRONZE STARLIGHT previously used this tool.

The path that the NPS tool was operating from in this research shares similarities with BRONZE STARLIGHT's chosen path conventions. Table 2 below presents these similarities.

These folders exist by default in the operating system, so this is not sufficient evidence by itself to connect the related activity to this group or another. However, we believe that it is not coincidental that two ransomware groups use this uncommon tool and choose to place it under a similar path on infected environments, using the `update` suffix for both files.

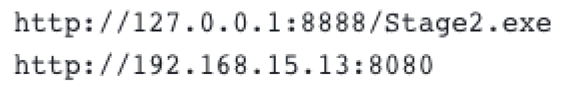
RA World	BRONZE STARLIGHT
C:\Windows\Help\ Windows\ContentStore\[redacted]_ **update**.exe	**C:\Windows\Help\** mui\0409\Windows**Update** .exe

Table 2. File path and naming convention similarities between the NPS tool variants deployed by RA World and BRONZE STARLIGHT.

- **Impacket use:** RA World used the same Impacket modules that Sygnia's report mentions, to facilitate reconnaissance and lateral movement.
- **Babuk use:** The latest final ransomware payload of both of the groups is based on Babuk's leaked source code.
- **VirusTotal submitter origin country:** When pivoting through VirusTotal and searching for files containing the string `C:\Windows\Help\Exclude.exe`, we noticed that the same submitter hailing from Hong Kong uploaded multiple variants of the `Stage1.exe` loader.

Some variants' code iterations look incomplete, and this strengthens our assumption that this might be the threat actor testing their arsenal for detection rates.

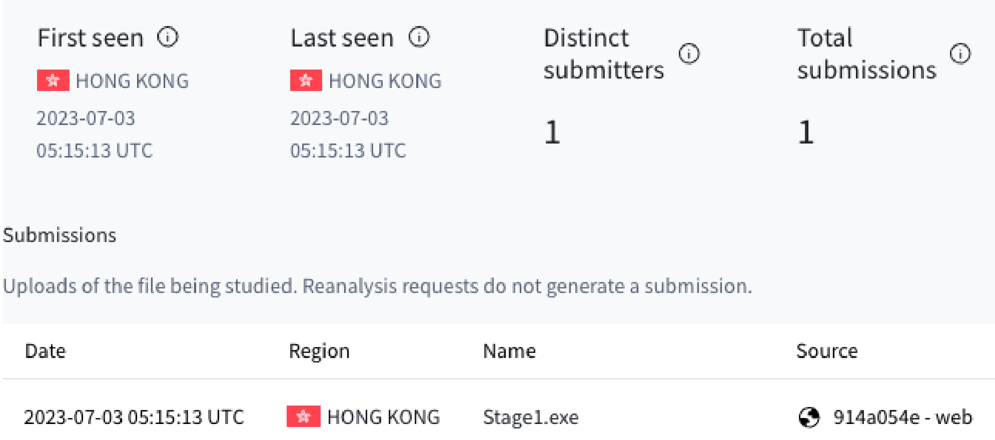
One variant included the two strings seen in Figure 14 below. These strings contained internal IP addresses, which did not exist in other samples. The presence of these strings also indicates that this is an early loader variant likely in a development phase.



```
http://127.0.0.1:8888/Stage2.exe
http://192.168.15.13:8080
```

Figure 14. IP strings from a presumed test variant of RA World's loader malware.

All the submissions had only one distinct submitter. This submitter uploaded one sample after another with a few minutes in between, on July 3, 2023. Figure 15 below shows the submitter information.



First seen
HONG KONG
2023-07-03
05:15:13 UTC

Last seen
HONG KONG
2023-07-03
05:15:13 UTC

Distinct submitters
1

Total submissions
1

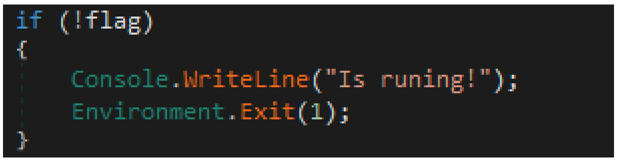
Submissions

Uploads of the file being studied. Reanalysis requests do not generate a submission.

Date	Region	Name	Source
2023-07-03 05:15:13 UTC	HONG KONG	Stage1.exe	914a054e - web

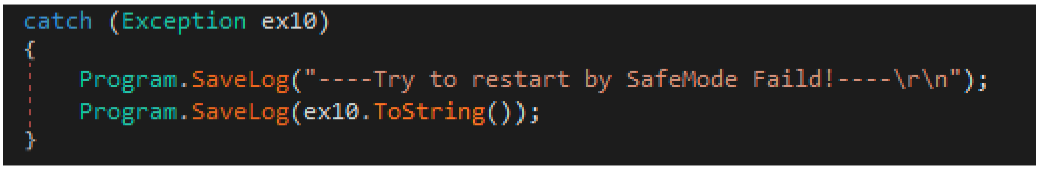
Figure 15. Submitter information from VirusTotal about the unique uploader of the loader files.

- **The threat actor's operating time zone:** Analyzing our telemetry, we noticed that threat actors executed the vast majority of reconnaissance and lateral movement-related commands on infected devices during office hours of the GMT +7 to GMT +9 time-zones.
- **Misspellings in the code:** While looking at the code of the different malware, we saw that logs by the author had clear mistakes in their use of English. Although it does not indicate a specific geographical location of an author, combining this finding together with other aforementioned points indicates that the threat developers are likely not native English speakers.Figures 16 and 17 below show examples of misspellings.



```
if (!flag)
{
    Console.WriteLine("Is runing!");
    Environment.Exit(1);
}
```

Figure 16. A first example of a typo in RA World's code.



```
catch (Exception ex10)
{
    Program.SaveLog("----Try to restart by SafeMode Faild!----\r\n");
    Program.SaveLog(ex10.ToString());
}
```

Figure 17. A second example of a typo in RA World's code.

However, it is important to note that there could be other explanations for the connections described here. For example, other threat actors might coincidentally use Babuk or some of the same open source tooling, and threat actors from other countries might be prone to the same types of misspellings. Therefore, while the possible ties to BRONZE STARLIGHT bring up intriguing possibilities, we assess the connection with low confidence at this time.

Conclusion

In this article, we reviewed the latest developments in the operation of RA World that has recently rebranded itself from RA Group. We described evolutions in both their leak site and their operational tools. They used two different loaders to deliver their final payload, which was a new variant of the Babuk ransomware.

The RA World group remains steadily active, and they primarily affect the manufacturing sector according to their public leak site data.

Protections and Mitigations

Palo Alto Networks customers are better protected from the different TTPs used by RA World.

The Cortex XDR and XSIAM platforms detect and prevent the execution flows described in the screenshots included in the previous sections. Cortex Xpanse is able to provide visibility that can prove valuable for proactive protection.

The Cortex XDR agent included out of the box protections that prevented adverse behavior from the samples we tested from this group, without the need for specific detection logic or signatures.

Cortex XDR and XSIAM detect user- and credential-based threats by analyzing user activity from multiple data sources including the following:

- Endpoints
- Network firewalls
- Active Directory
- Identity and access management solutions
- Cloud workloads

Cortex XDR and XSIAM build behavioral profiles of user activity over time with machine learning. By comparing new activity to past activity, peer activity and the expected behavior of the entity, Cortex XDR and XSIAM detect anomalous activity indicative of credential-based attacks.

They are also designed offer the following protections related to the attacks discussed in this post:

- Preventing the execution of known malicious malware
- Preventing execution of unknown malware using Behavioral Threat Prevention and machine learning based on the Local Analysis module
- Protecting against credential-gathering tools and techniques using the Credential Gathering Protection, available from Cortex XDR 3.4
- Protecting against exploitation of different vulnerabilities including ProxyShell using the Anti-Exploitation modules as well as Behavioral Threat Protection

Cortex XDR is designed to detect post-exploitation activity, including credential-based attacks, with behavioral analytics.

The Prisma Cloud Defender as well as Cortex XDR for cloud agents should be deployed on cloud-based Windows virtual machines to ensure they are protected from these known malicious binaries. Advanced WildFire signatures can be used by both Palo Alto Networks cloud services to ensure cloud-based Windows virtual machine runtime operations are being analyzed and those resources are protected.

Cloud-Delivered Security Services for the Next-Generation Firewall such as Advanced WildFire and Advanced URL Filtering include protections based on the IoCs shared in this article.

If you think you might have been impacted or have an urgent matter, get in touch with the Unit 42 Incident Response team or call:

- North America Toll-Free: 866.486.4842 (866.4.UNIT42)
- EMEA: +31.20.299.3130
- APAC: +65.6983.8730
- Japan: +81.50.1790.0200

Palo Alto Networks has shared these findings with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

Indicators of Compromise

Examples of Stage 1

- `2a4e83ff1c48baa3d526d51d09782933cec6790d5fa8ccea07633826f378b18a`
- `57225f38b58564cf7ec1252fbf12475abee58bd6ea9500eb7570c49f8dc6a64c`
- `93aae0d740df62b5fd57ac69d7be75d18d16818e87b70ace5272932aa44f23e4`
- `af4a08bbe9f698a8a9666c76c6bdac9a29b7a9572e025f85f2a6f62c293c0f5e`
- `f1c576ed08abbb21d546a42a0857a515d617db36d2e4a49bedd9c25034ccd1e2`

Examples of Stage 2

- `2d22cbe3b1d13af824d10bb55b61f350cb958046adf5509768a010df53409aa8`
- `330730d65548d621d46ed9db939c434bc54cada516472ebef0a00422a5ed5819`

Examples of Stage 3 (Babuk Variant)

- `9479a5dc61284ccc3f063ebb38da9f63400d8b25d8bca8d04b1832f02fac24de`
- `31ac190b45cc32c04c2415761c7f152153e16750516df0ce0761ca28300dd6a4`
- `74fb402bc2d7428a61f1ac03d2fb7c9ff8094129afd2ec0a65ef6a373fd31183`
- `7c14a3908e82a0f3c679402cf060a0bcae7791bdc25715a49ee7c1fc08215c93`
- `817b7dab5beba22a608015310e918fc79fe72fa78b44b68dd13a487341929e81`
- `8e4f9e4c2bb563c918fbe13595de9a32b307e2ce9f1f48c06b168dbbb75b5e89`
- `bb63887c03628a3f001d0e93ab60c9797d4ca3fb78a8d968b11fc19da815da2f`
- `d0c8dc7791e9462b6741553a411a5bfa5f4a9ad4ffcf91c0d2fc3269940e48a2`
- `d311674e5e964e7a2408b0b8816b06587b2e669221f0e100d4e0d4a914c6202c`

- `25ba2412cf0b97353fa976f99fdd2d9ecbbe1c10c1b2a62a81d0777340ce0f0a`
- `31105fb81a54642024ef98921a524bf70dec655905ed9a2f5e24ad503188d8ae`
- `826f05b19cf1773076a171ef0b05613f65b3cc39a5e98913a3c9401e141d5285`
- `36ce5b2c97892f86fd0e66d9dd6c4fbd4a46e7f91ea55cc1f51dee3a03417a3a`
- `108a3966b001776c0cadac27dd9172e506069cb35d4233c140f2a3c467e043d0`
- `bc2caec044efe0890496c56f29d7c73e3915740bc5fda7085bb2bb89145621e5`
- `1066395126da32da052f39c9293069f9bcc1c8d28781eb9d44b35f05ce1fd614`
- `b2b59f10e6bdbe4a1f8ff560dbfe0d9876cbb05c7c27540bd824b17ceb082d62`
- `4392dcce97df199e00efb7a301e26013a44ee79d9b4175d4539fae9aed4f750b`
- `e31f5ebff2128decd36d24af7e155c3011a9afdc36fd14480026de151e1ecee2`
- `0183edb40f7900272f63f0392d10c08a3d991af41723ecfd38abdfbfdf21de0a`

Additional References

- Newly identified RA Group compromises companies in U.S. and South Korea with leaked Babuk source code – Talos Intelligence, Cisco
- Multistage RA World Ransomware Uses Anti-AV Tactics, Exploits GPO – Trend Micro
- New RA Group ransomware gang is the latest group using leaked Babuk source code – Security Affairs
- Explore the SAM hive with Regedit (and Sysinternals) – Cyber Defence Lab of the Royal Military Academy (Belgium)
- Understanding NTDS.DIT: The Core of Active Director – Harikrishnan P. on Medium
- Germán Fernández @1ZRR4H on X (formerly Twitter)
- How To Detect SYSVOL Enumeration Exploits – Blumira
- BRONZE STARLIGHT (Threat Actor) – Malpedia
- Revealing Emperor Dragonfly: Night Sky and Cheerscrypt - A Single Ransomware Group – Sygnia
- Mutation Effect of Babuk Code Leakage: New Ransomware Variants – SOCRadar