

MAGNIBER'S MISSTEPS:

BECAUSE EVEN SPIDERS TRIP OVER THEIR OWN WEB

Amata, Patrik, Kim

AGENDA

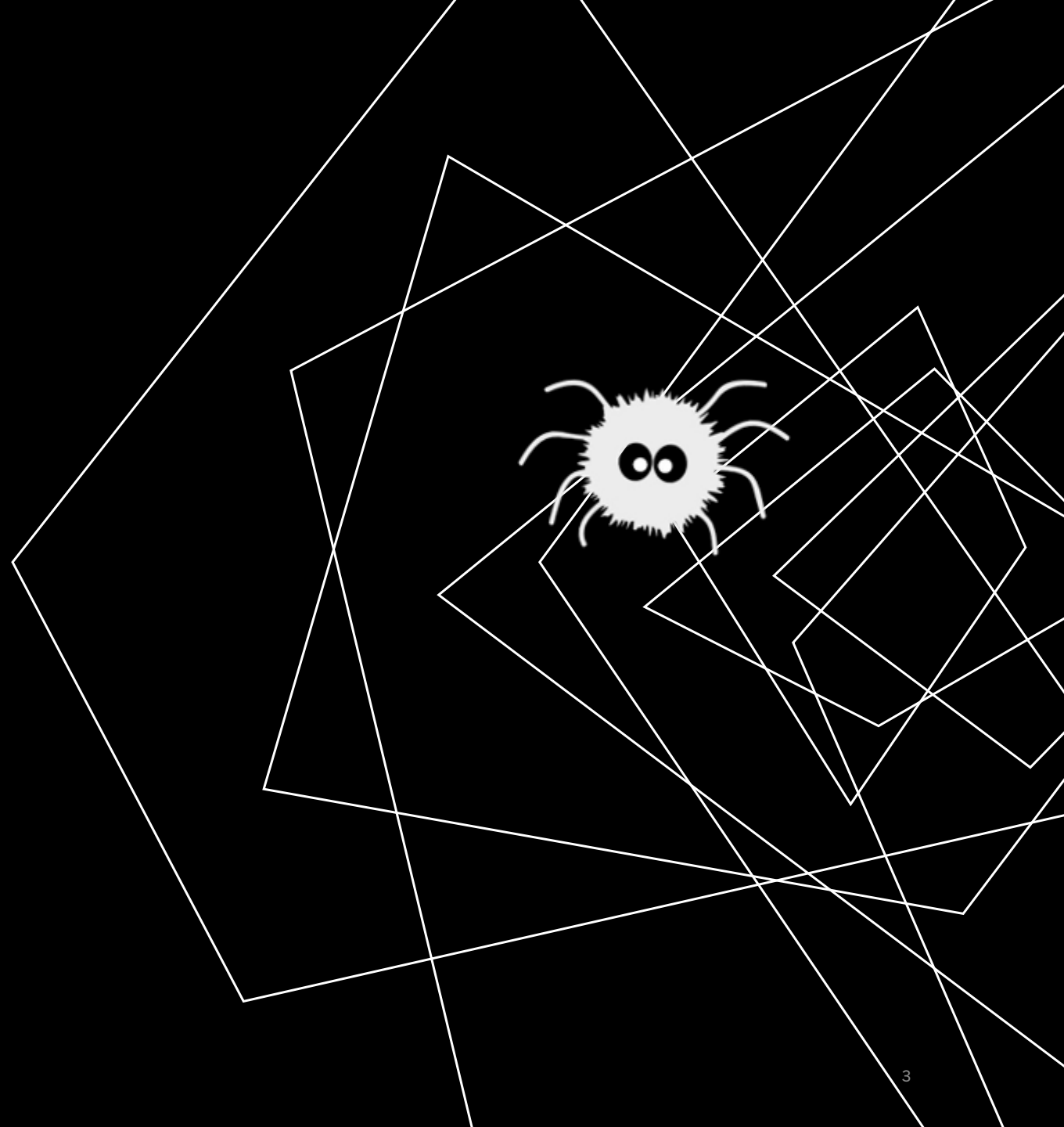
Who is Magniber?

Misconfigured Servers

- Leaked PHP script
- Victim logs
- RSA Private keys

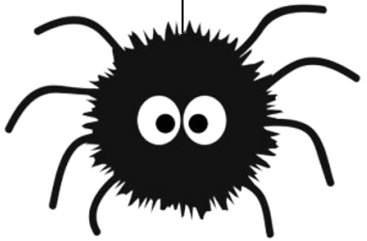
Summary

Q&A

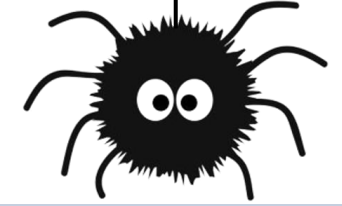


MAGNIBER

- Operating since 2017
- Targeting East Asia, mostly Taiwan and South Korea
- Using sophisticated techniques to infect their victims
 - 0day vulnerabilities in Microsoft SmartScreen (CVE-2023-24880, CVE-2022-44698)
- Targeting European countries early this year



THE HUNT



C2 (Command and Control) server



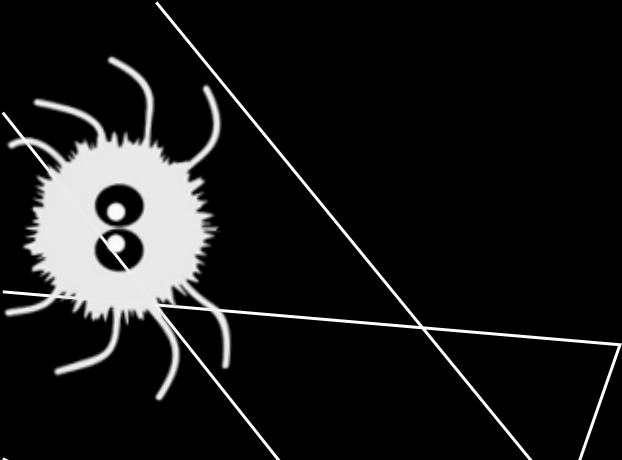
```
51.77.24.186
MyHosti Server
France, Argenteuil

HTTP/1.1 200 OK
Date: Mon, 23 Jan 2023 19:11:53 GMT
Server: Apache
Last-Modified: Fri, 20 Jan 2023 22:14:27 GMT
ETag: "4a1e-5f2b95f66d6c0"
Accept-Ranges: bytes
Content-Length: 18974
Connection: close

<?
error_reporting(0);
ini_set('display_errors',0);

$domains[] = 'agehim.email';
$doma...
```

86 servers



DIVING INTO THE PHP SCRIPT

Serves the Magniber ransomware (locker) to victims

```
285 function getmsicontent()  
286 {  
287     $msipath = '/home/dima/content/msi/';  
288  
289     if (date("i") < 15) $partmin = '0';  
290     else if ((date("i") > 14) && (date("i") < 30)) $partmin = '1';  
291     else if ((date("i") > 29) && (date("i") < 45)) $partmin = '2';  
292     else if (date("i") > 44) $partmin = '3';  
293  
294     $pathfmsi = $msipath . 'ver' . sprintf("%02d", date("H")) . '_' . $partmin . '.msi';
```

Payload rotates every 15 min



DIVING INTO THE PHP SCRIPT

```
5 $domains[] = 'agehim.email';
6 $domains[] = 'balltoo.email';
7 $domains[] = 'bitmap.email';
8 $domains[] = '.....';
9 $domains[] 18 if (date("H") < 2) $domnum = 0;
10 $domains[] 19 else if ((date("H") >= 2) && (date("H") < 4)) $domnum = 1;
11 $domains[] 20 else if ((date("H") >= 4) && (date("H") < 6)) $domnum = 2;
12 $domains[] 21 else if ((date("H") >= 6) && (date("H") < 8)) $domnum = 3;
13 $domains[] 22 else if ((date("H") >= 8) && (date("H") < 10)) $domnum = 4;
14 $domains[] 23 else if ((date("H") >= 10) && (date("H") < 12)) $domnum = 5;
15 $domains[] 24 else if ((date("H") >= 12) && (date("H") < 14)) $domnum = 6;
16 $domains[] 25 else if ((date("H") >= 14) && (date("H") < 16)) $domnum = 7;
17 $domains[] 26 else if ((date("H") >= 16) && (date("H") < 18)) $domnum = 8;
18 $domains[] 27 else if ((date("H") >= 18) && (date("H") < 20)) $domnum = 9;
19 $domains[] 28 else if ((date("H") >= 20) && (date("H") < 22)) $domnum = 10;
20 $domains[] 29 else if ((date("H") >= 22) && (date("H") < 24)) $domnum = 11;
21 $domains[] 30 $firstdomain = $domains[$domnum];
```

- List of 12 domains
- Each domain is active for 2 hours

atures



DIVING INTO THE PHP SCRIPT

created	domain	registrar	isp
2023-02-06T23:20:33	blowoh.email	NameSilo, LLC	OVH-MNT
2023-02-06T23:20:34	hidesat.email	NameSilo, LLC	OVH-MNT

created	domain	registrar	isp
2023-02-06T23:20:33	blowoh.email	NameSilo, LLC	T
2023-02-06T23:20:34	hidesat.email	NameSilo, LLC	T
2023-02-06T23:20:35	gotmod.email	NameSilo, LLC	T
2023-02-06T23:20:36	madan.email	NameSilo, LLC	T
2023-02-06T23:20:36	quieta.email	NameSilo, LLC	T
2023-02-06T23:20:37	tanksa.email	NameSilo, LLC	T
2023-02-06T23:20:38	cycleso.email	NameSilo, LLC	T
2023-02-06T23:20:39	sixhung.email	NameSilo, LLC	T
2023-02-06T23:20:40	bighead.email	NameSilo, LLC	T
2023-02-06T23:20:40	fishswe.email	NameSilo, LLC	T
2023-02-06T23:20:41	tenweek.email	NameSilo, LLC	T
2023-02-06T23:20:42	betsdry.email	NameSilo, LLC	T

2023-02-07T23:33:16	moveeye.email	NameSilo, LLC	OVH-MNT
2023-02-07T23:33:17	isfed.email	NameSilo, LLC	OVH-MNT
2023-02-07T23:33:18	maytwo.email	NameSilo, LLC	OVH-MNT
2023-02-07T23:33:19	heboxs.email	NameSilo, LLC	OVH-MNT
2023-02-07T23:33:20	naiveoh.email	NameSilo, LLC	OVH-MNT

- List of 12 domains
- Each domain is active for 2 hours
- Changes every day. Why?
 - Outpace domain-based signatures
 - Anti-analysis?
- Domain Generation Algorithm
 - How identify?
- Automated domain registration
- Registrar NameSilo, BTC



DIVING INTO THE PHP SCRIPT

Jan 2023: Targeting European countries

```
$allowedcountries = array("DE", "FR", "IT", "BE", "NL", "DK", "AT", "CH", "NO", "SE", "FI");
```

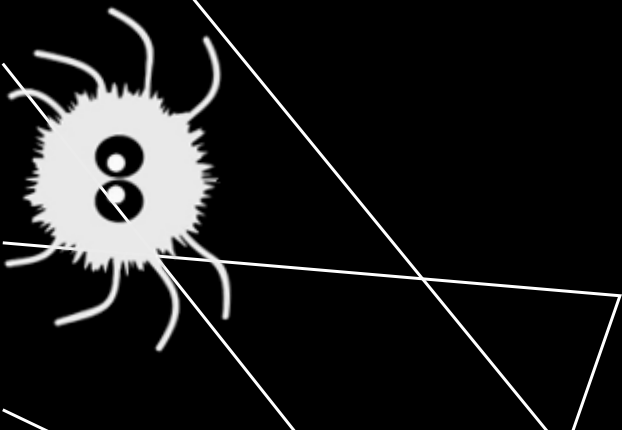
Feb 2023: Targeting South Korea & Taiwan

```
$allowedcountries = array("KR", "KO", "TW");
```

Filters to prevent analysis

- Reverse DNS, User-Agent, Referrer, ...

```
$blocked_country = array("A1", "A2", "O1", "SU", "RU", "UA", "BY", "UZ",  
"KZ", "GE", "AZ", "KG", "TJ", "AM", "TM", "JP", "JA"); //,"JA","CN","ZH"
```

DIVING INTO THE PHP SCRIPT

Payload names

```
// $fname = "SYSTEM.Critical.Upgrade.Win10.0." . substr(md5($_SERVER["REMOTE_ADDR"]), 0, rand(12,16)) . ".msi";  
// $fname = "ALERT." . substr(md5($_SERVER["REMOTE_ADDR"]), 0, rand(12,16)) . ".msi";  
// $fname = "Antivirus.Update.Cloud." . substr(md5($_SERVER["REMOTE_ADDR"]), 0, rand(12,16)) . ".msi";  
// $zipname = "SYSTEM.Critical.Upgrade.Win10.0." . substr(md5($_SERVER["REMOTE_ADDR"]), 0, rand(12,16)) . ".zip";  
// $fname = "Antivirus.Update.Cloud." . substr(md5($_SERVER["REMOTE_ADDR"]), 0, rand(12,16)) . ".msi";  
// $zipname = "Antivirus.Update.Cloud." . substr(md5($_SERVER["REMOTE_ADDR"]), 0, rand(12,16)) . ".zip";  
// $fname = "SYSTEM.Antivirus.Update." . substr(md5($_SERVER["REMOTE_ADDR"]), 0, rand(12,16)) . ".msi";  
// $zipname = "SYSTEM.Antivirus.Update." . substr(md5($_SERVER["REMOTE_ADDR"]), 0, rand(12,16)) . ".zip";  
// $fname = "SYSTEM.Critical.Upgrade.Win10.0." . substr(md5($_SERVER["REMOTE_ADDR"]), 0, rand(12,16)) . ".msi";  
// $zipname = "SYSTEM.Critical.Upgrade.Win10.0." . substr(md5($_SERVER["REMOTE_ADDR"]), 0, rand(12,16)) . ".zip";  
$fname = "MS.Update.Center.Security.KB" . rand(111111, 99999999) . ".msi";  
$zipname = "MS.Update.Center.Security.KB" . rand(111111, 99999999) . ".zip";  
// $fname = "ERROR.Software.Log." . md5($_SERVER["REMOTE_ADDR"]) . ".msi";  
// $zipname = "ERROR.Software.Log." . rand(111111, 99999999) . ".zip";  
// $fname = "COVID.Warning.Readme." . md5($_SERVER["REMOTE_ADDR"]) . ".msi";  
// $zipname = "COVID.Warning.Readme." . md5($_SERVER["REMOTE_ADDR"]) . ".zip";  
// $fname = "Antivirus.Upgrade.Database.Cloud.msi";  
// $zipname = "Antivirus.Upgrade.Database.Cloud.zip";
```



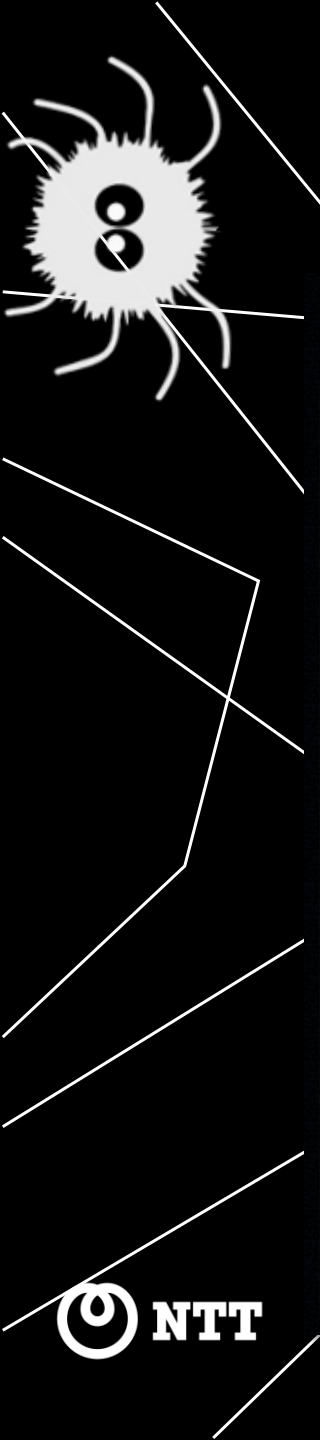
SHODAN REMEMBERS

Historical data on Shodan

Query → Timeline

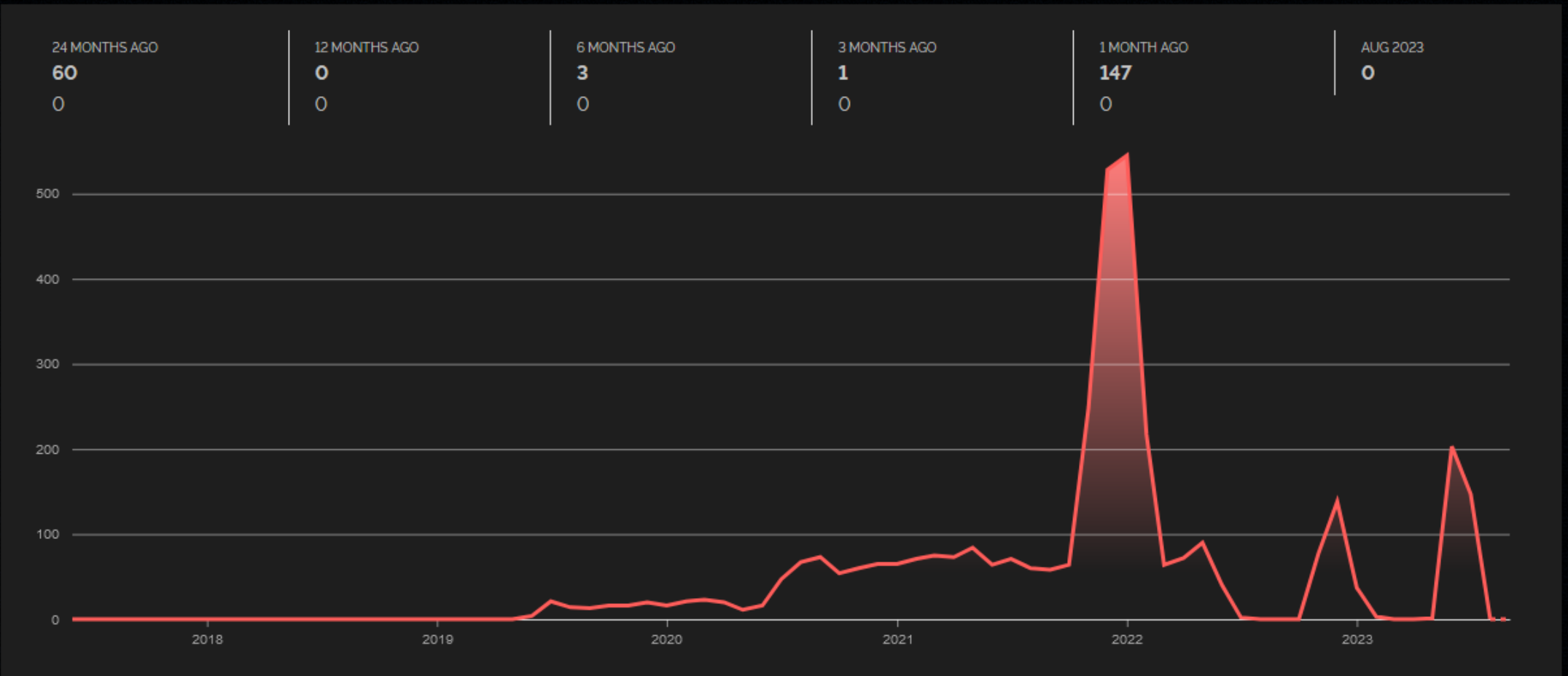
Unique keyword?

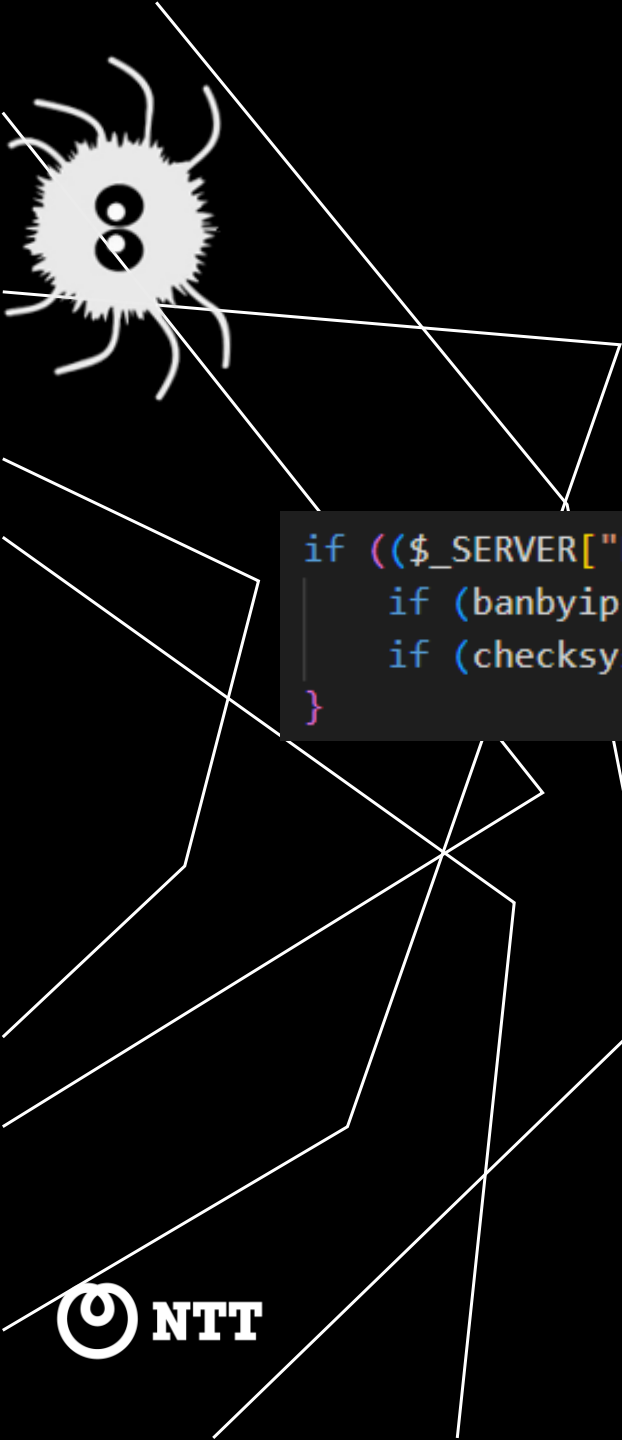
```
41  define("DBName", "general");  
42  define("HostName", "localhost");  
43  define("UserName", "dimak");  
44  define("Password", "NESpEp5PunEnA6a1Rl01");
```



SHODAN REMEMBERS

"NESpEp5PunEnA6a1Rl01"





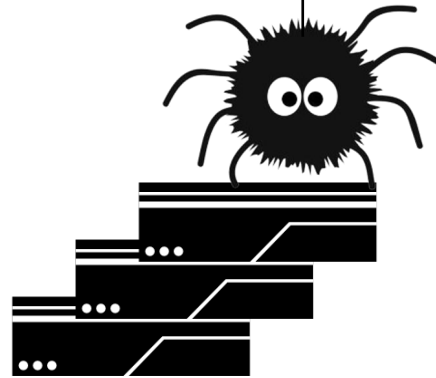
DIVING INTO THE PHP SCRIPT

- Two hosts are excluded from anti-bot/filter checks:

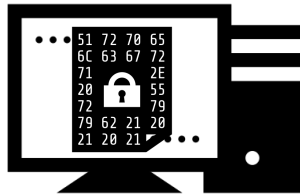
```
if (($_SERVER["REMOTE_ADDR"] != '95.217.220.23') && ($_SERVER["REMOTE_ADDR"] != '70.34.195.240')) {  
    if (banbyip()) err404();  
    if (checksystem()) err404();  
}
```

- Likely used by TA
 - Testing payloads?
 - Managing infrastructure?
- “Jump hosts”

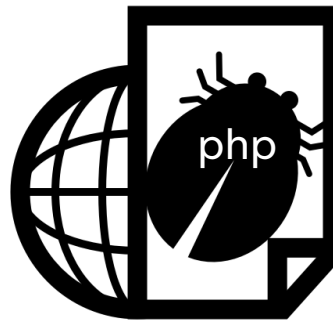
INFRASTRUCTURE



~300 hosts
~440 HTTP services



Victim



86 misconfigured servers
Payload delivery



2 jump hosts

THE HUNT CONTINUE..



TOTAL RESULTS

442

TOP COUNTRIES

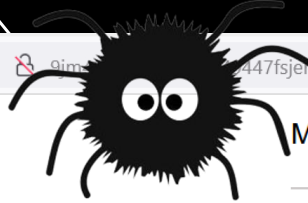


TOP PORTS

80	304
443	136
8080	1



Exposing log file



MY DECRYPTOR

[Home Page](#)

[Support](#)

[Decrypt 1 file for FREE](#)

[Decryption FAQ](#)

[Reload current page](#)

Your documents, photos, databases and other important files have been ENCRYPTED !

WARNING! Any attempts to restore your files with the third-party software will be fatal for your files! **WARNING!**

To decrypt your files you need to buy the special software - "My Decryptor"

All transactions should be performed via **BITCOIN** network.

You can purchase this product at a special price within 5 days: **BTC 0.11 (~ \$2882)**

After 5 days the price of this product will increase up to: **BTC 0.4400 (~ \$11530)**

The special price is available:

04 . 08:25:36

DIVING INTO THE LOG

- Logged activities towards “My Decryptor”
- Divided in 6 types

Preland:

Victim information Exfiltration

Getdecrypt:

Downloaded decryptor

Lendstart:

Logged every time someone visits
”My Decryptor”

Chat:

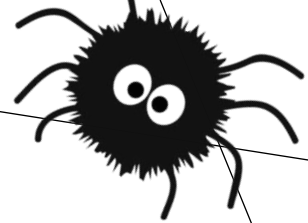
Victim messages in support chat

Freedecrypt:

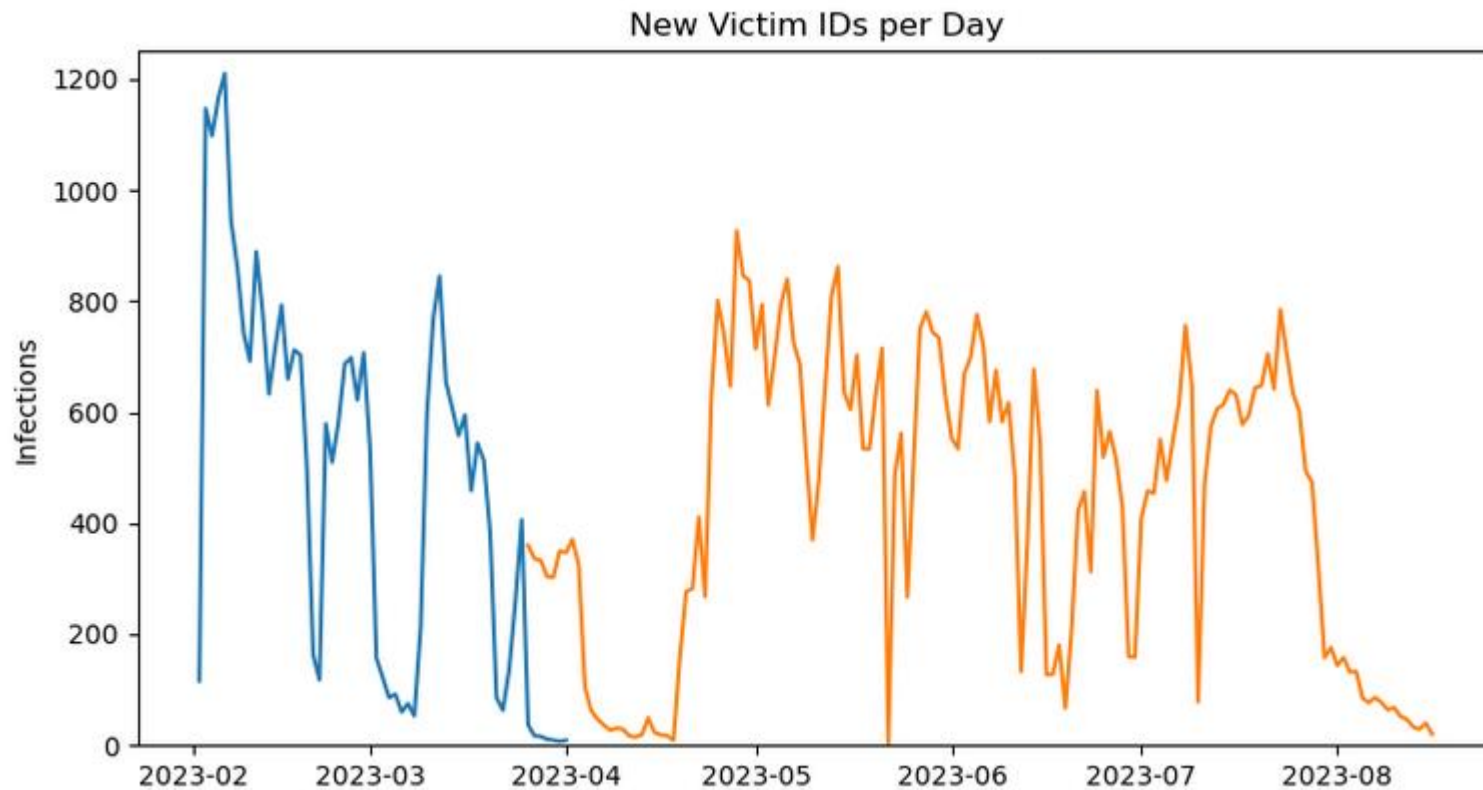
Upload file for free decryption

Getfreedecrypt:

Download decrypted test file



DIVING INTO THE LOG



2 log servers

- Migrated to 2nd server during April

89 000 victims

- 99 % victims are KR + TW
- European countries

DIVING INTO THE LOG

```
if (($_SERVER["REMOTE_ADDR"] != '95.217.220.23') && ($_SERVER["REMOTE_ADDR"] != '70.34.195.240')) {  
    if (banbyip()) err404();  
    if (checksystem()) err404();  
}
```

Observed jump host in the log as victim

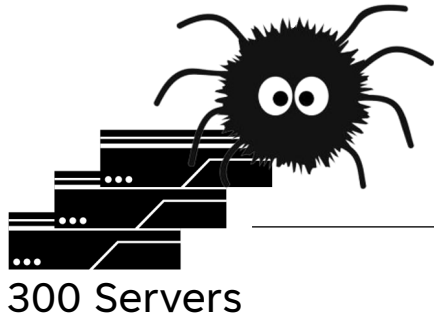
- Testing payloads

Based on analysis of *Getdecrypt* log type in correlation of data on the ransom page, we estimate the threat actor earned

- 16 BTC ~ 450 000 USD



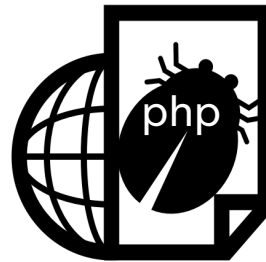
INFRASTRUCTURE (UPDATE)



Log server:8080



My Decryptor

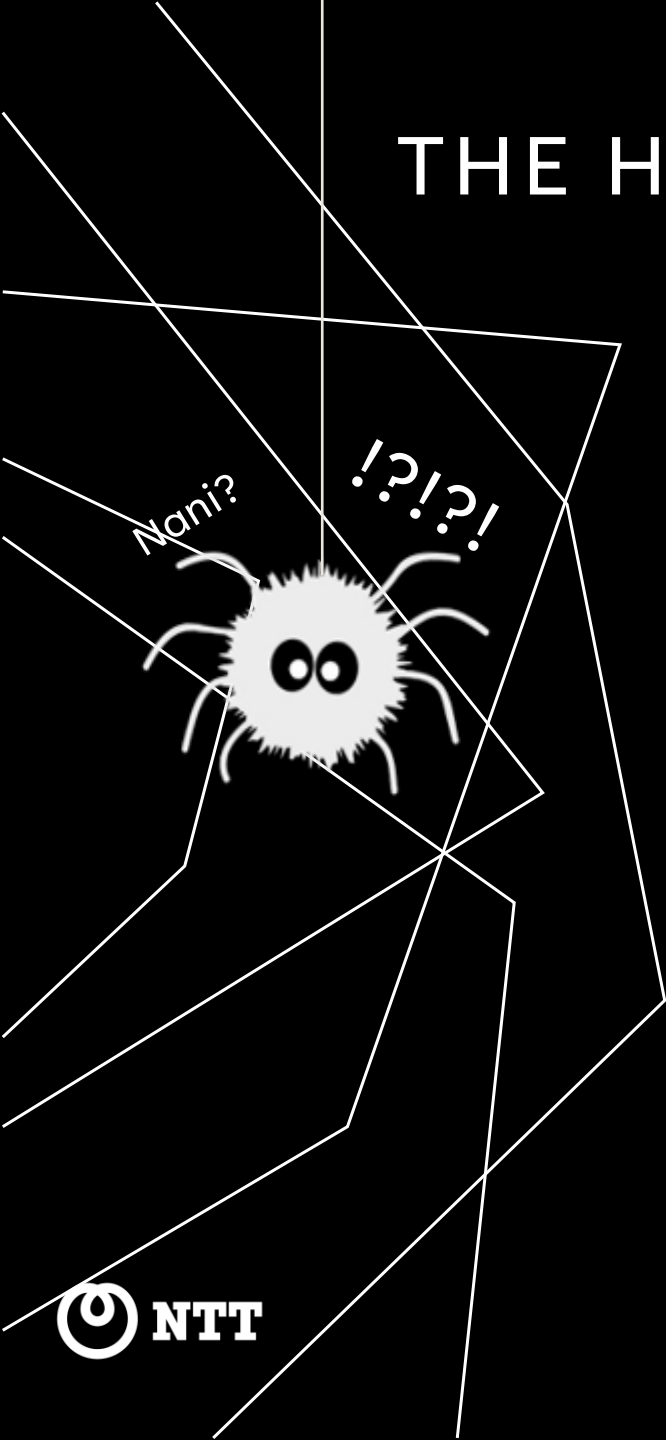


Ransomware delivery



Jump host

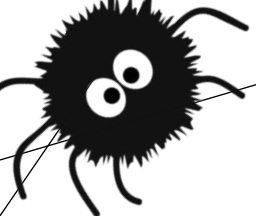
THE HUNT CONTINUE..



Log server:8080

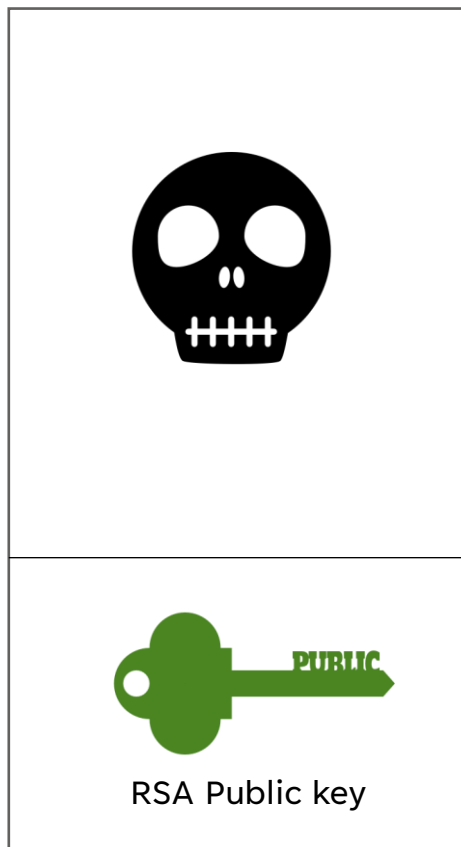


RSA Private key

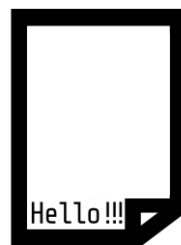


MAGNIBER ENCRYPTION LOGIC

Locker.msi

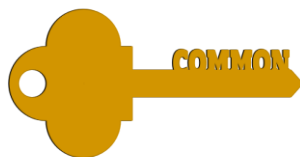


Generate



Diary.docx

Encrypt



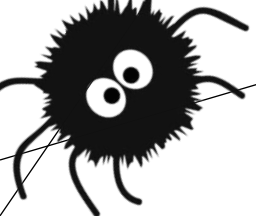
AES encrypted
with RSA pub

Encrypt

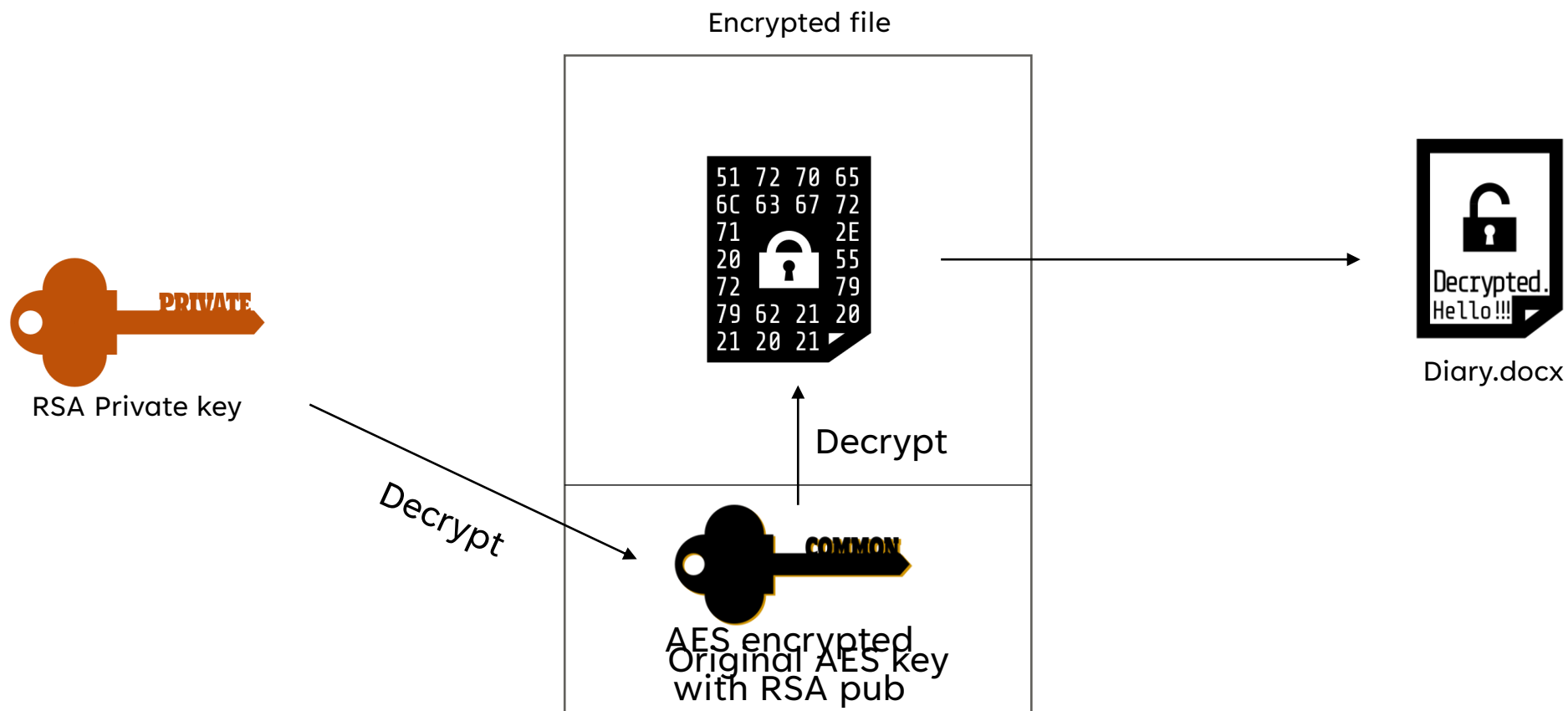
Append

Encrypted file





MAGNIBER DECRYPTION LOGIC



POC



Magniber Decryptor

172.16.1.5:5000

130%

MAGNIBER DECRYPTOR

Drop an encrypted file here or click to browse

encrypted

New

Sort

View

Search encrypted

Earlier this year

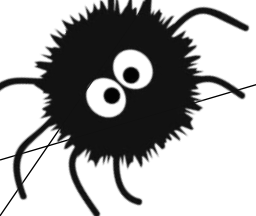
Document_pdf.abcdef

Document_xls.abcdef

2 items

NTT

16:48 2023-09-30



HOW MANY VICTIMS COULD BE DECRYPTED?

PHP script: A different locker is delivered every 15 min

Exposed log: 6 new victims in each 15 min interval

➔ Every key can roughly decrypt 6 victims

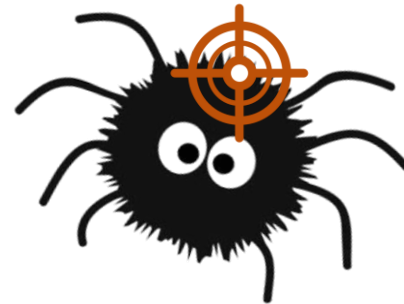
The RSA private key exposed when someone **paid** the ransom

We have collected **177** keys

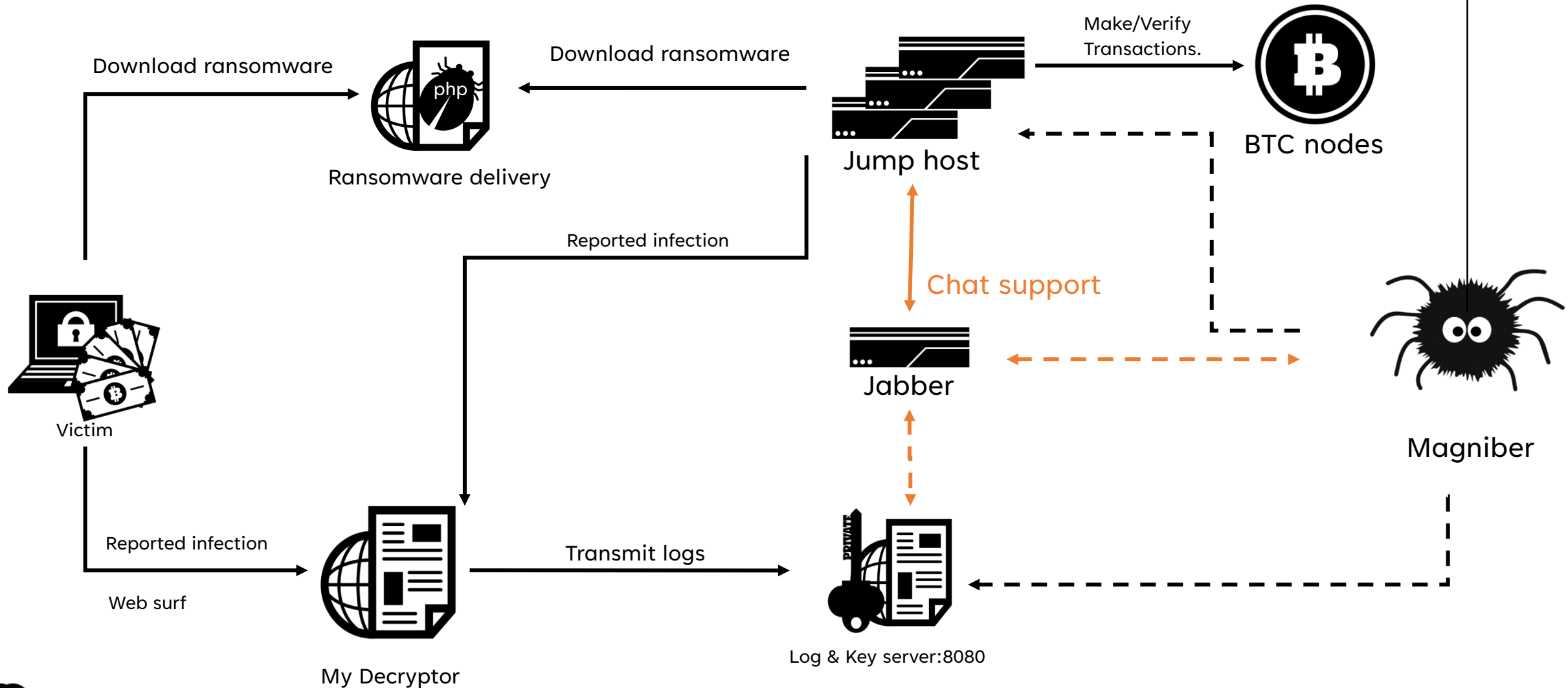


THREAT INTEL FROM NTT

- Derived threat intelligence data from NTT on the 2 jump hosts
- BTC nodes
 - Checking if the ransom has been paid
 - Paying for infrastructure
- Jabber server, “thesecure.biz”
 - Support chat



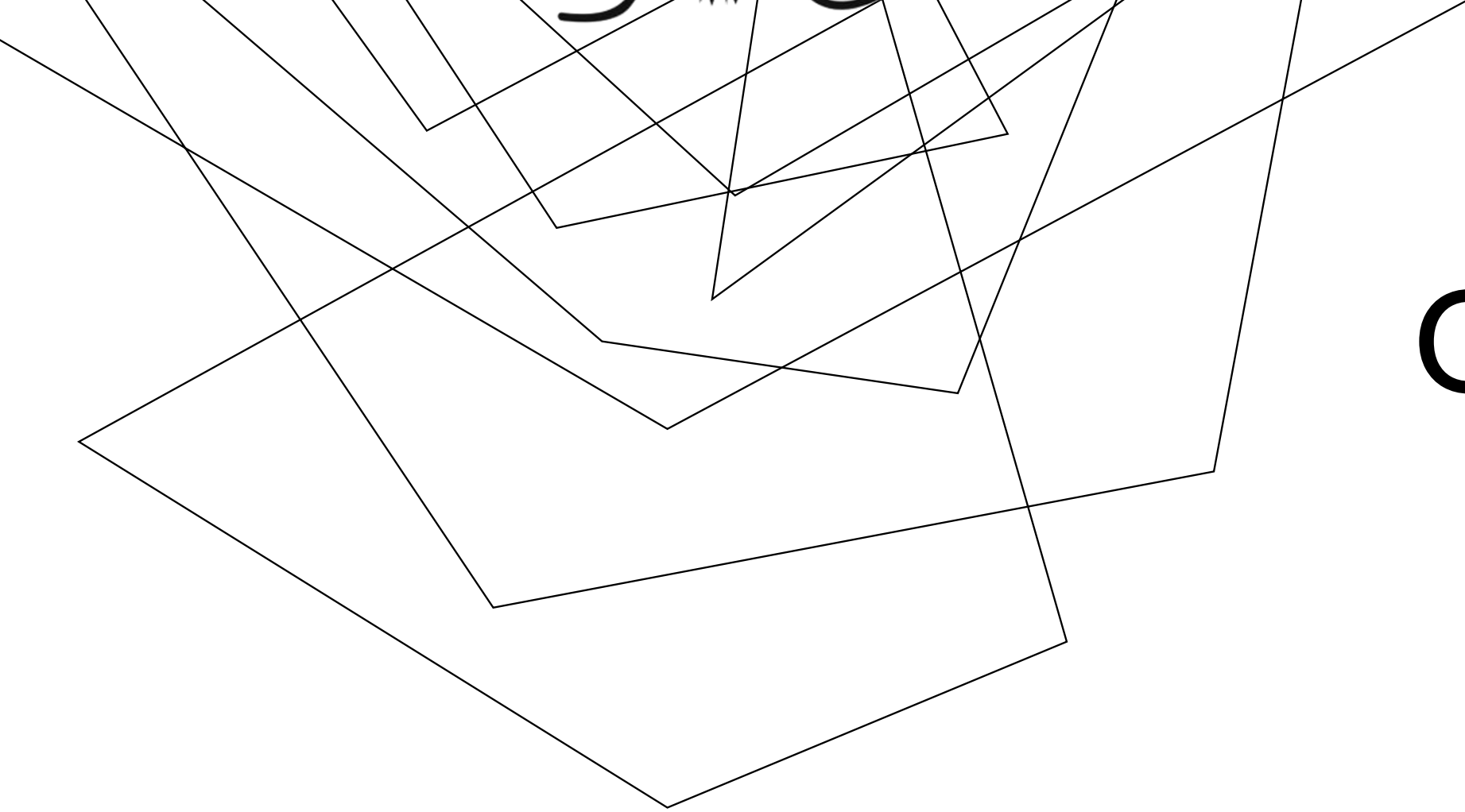
SPIDER WEB



SUMMARY

- Evade detection
 - DGA, 0days
- != Securing their Infra
- 89 000 victim
- 16 BTC
- <https://tinyurl.com/VB23-Magniber>
 - IoCs
 - RSA keys
 - BTC addresses



A series of thin, black, overlapping lines forming various geometric shapes like triangles and polygons, creating a complex, abstract pattern in the upper left portion of the slide.

Q&A

REFERENCES

- <https://blog.google/threat-analysis-group/magniber-ransomware-actors-used-a-variant-of-microsoft-smartscreen-bypass/>
- <https://asec.ahnlab.com/en/44315/>
- <https://hshrzd.wordpress.com/2023/03/30/magniber-ransomware-analysis/>
- <https://twitter.com/AvastThreatLabs/status/1613248556428582916>

