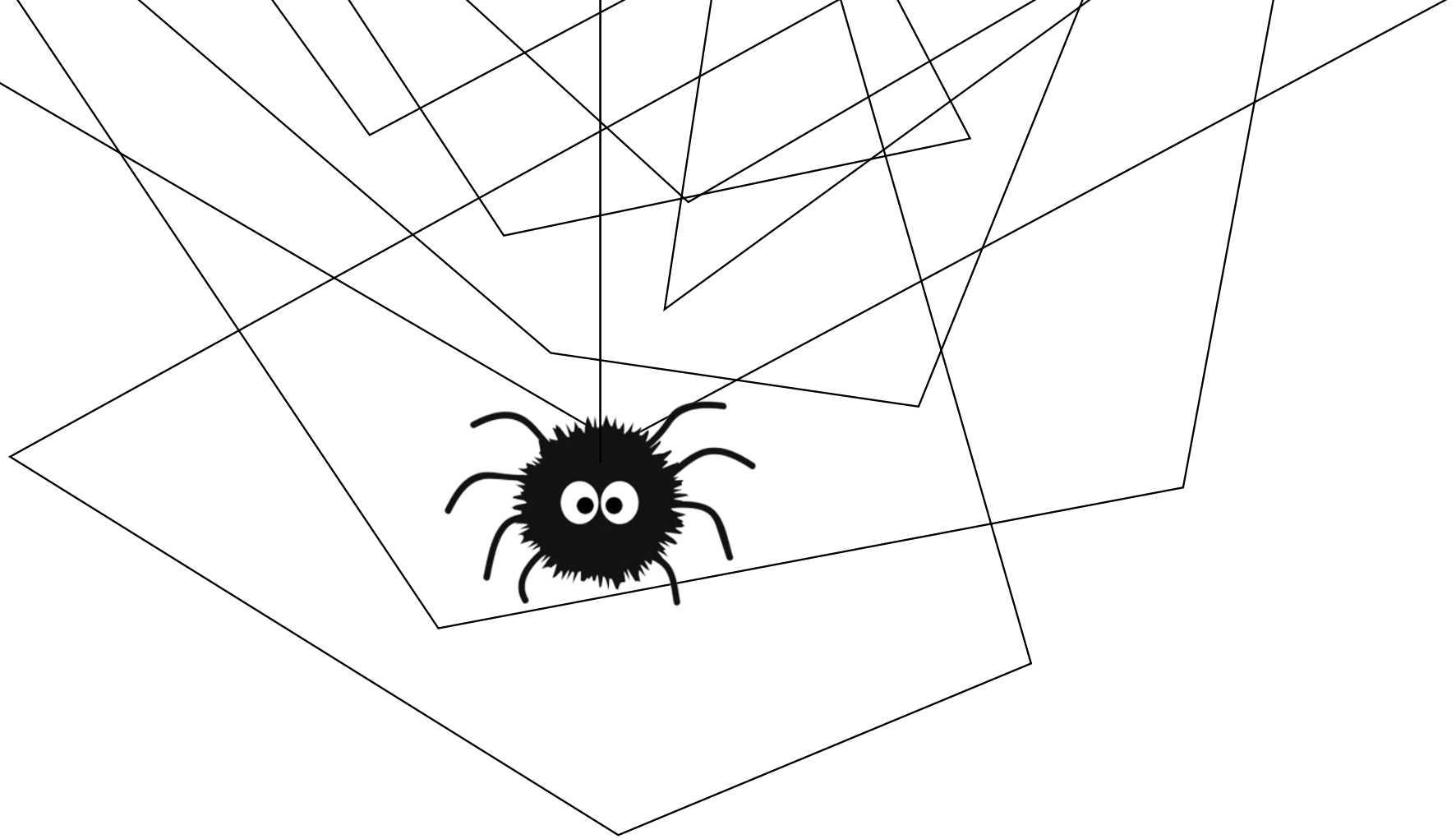


MAGNIBER'S MISSTEPS:

BECAUSE EVEN SPIDERS TRIP OVER THEIR OWN WEB

Amata, Patrik, Kim

NTT

AGENDA

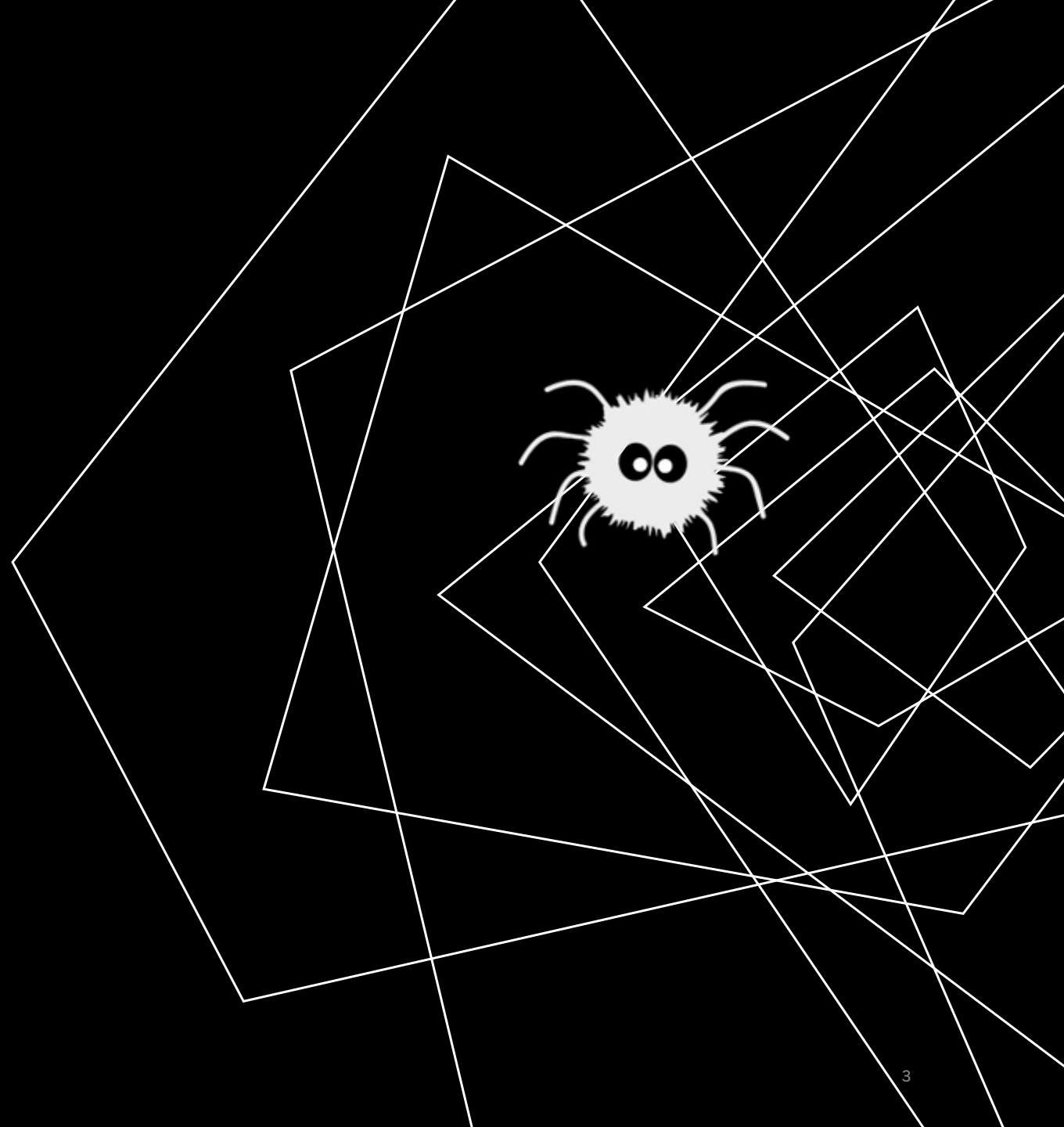
Who is Magniber?

Misconfigured Servers

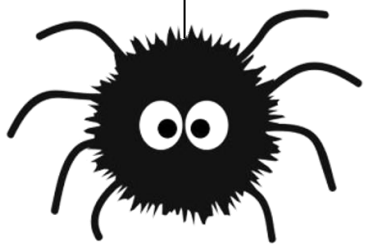
- Leaked PHP script
- Victim logs
- RSA Private keys

Summary

Q&A



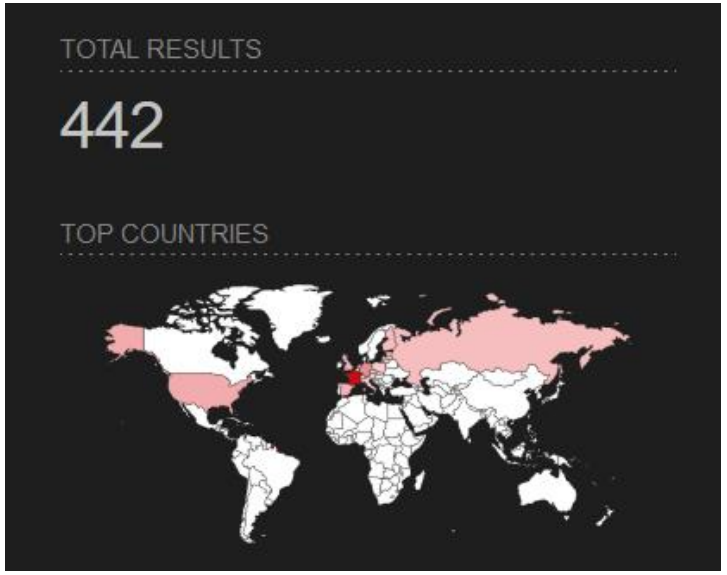
MAGNIBER

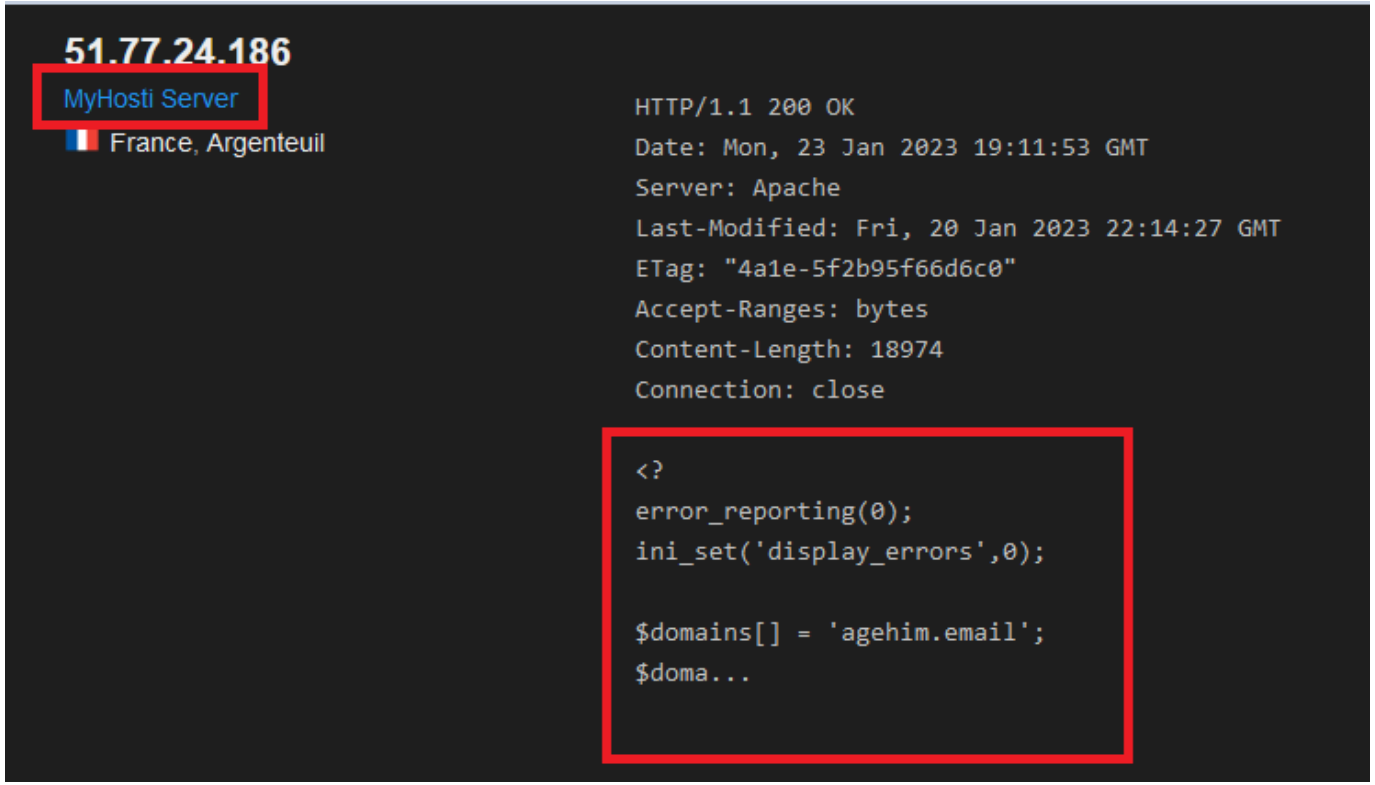


- Operating since 2017
- Targeting East Asia, mostly Taiwan and South Korea
- Using sophisticated techniques to infect their victims
  - 0day vulnerabilities in Microsoft SmartScreen (CVE-2023-24880, CVE-2022-44698)
- Targeting European countries early this year

THE HUNT

Web server





86 servers

NTT

DIVING INTO THE PHP SCRIPT

Serves the Magniber ransomware (locker) to victims

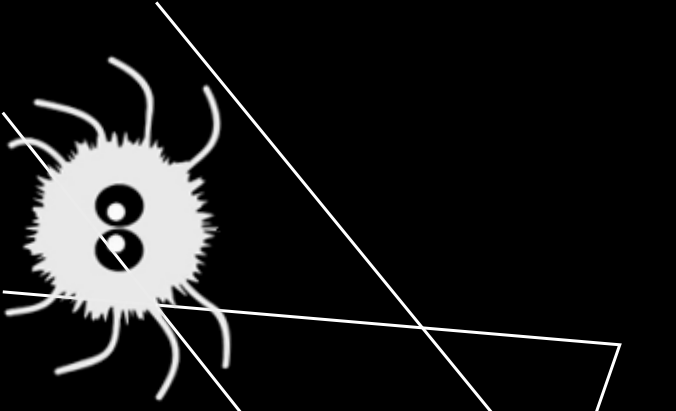
```
285  function getmsicontent()
286  {
287      $msipath = '/home/dima/content/msi/';
288
289      if (date("i") < 15) $partmin = '0';
290      else if ((date("i") > 14) && (date("i") < 30)) $partmin = '1';
291      else if ((date("i") > 29) && (date("i") < 45)) $partmin = '2';
292      else if (date("i")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

Payload rotates every 15 min

DIVING INTO THE PHP SCRIPT

```php
$domains[] = 'agehim.email';
$domains[] = 'balltoo.email';
$domains[] = 'bitsmap.email';
$domains[] = 'yeswash.email';
$domains[] = 'banlink.email';
$domains[] = 'bemoves.email';
$domains[] = 'fanfelt.email';
$domains[] = 'fantune.email';
$domains[] = 'itsair.email';
$domains[] = 'pipecry.email';
$domains[] = 'thelost.email';
$domains[] = 'wonnote.email';
```

- List of 12 domains



DIVING INTO THE PHP SCRIPT

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

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

DIVING INTO THE PHP SCRIPT

```
5    $domains[] = 'agehim.email';
6    $domains[] = 'balltoo.email';
7    $domains[] = 'bitsmap.email';
8    $domains[] = 'yeswash.email';
9    $domains[] = 'banlink.email';
10   $domains[] = 'bemoves.email';
11   $domains[] = 'fanfelt.email';
12   $domains[] = 'fantune.email';
13   $domains[] = 'itsair.email';
14   $domains[] = 'pipecry.email';
15   $domains[] = 'thelost.email';
16   $domains[] = 'wonnote.email';
```

- 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?

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
2023-02-06T23:20:35	gotmod.email	NameSilo, LLC	OVH-MNT
2023-02-06T23:20:36	madan.email	NameSilo, LLC	OVH-MNT
2023-02-06T23:20:36	quieta.email	NameSilo, LLC	OVH-MNT
2023-02-06T23:20:37	tanksa.email	NameSilo, LLC	OVH-MNT
2023-02-06T23:20:38	cycleso.email	NameSilo, LLC	OVH-MNT
2023-02-06T23:20:39	sixhung.email	NameSilo, LLC	OVH-MNT
2023-02-06T23:20:40	bighead.email	NameSilo, LLC	OVH-MNT
2023-02-06T23:20:40	fishswe.email	NameSilo, LLC	OVH-MNT
2023-02-06T23:20:41	tenweek.email	NameSilo, LLC	OVH-MNT
2023-02-06T23:20:42	betsdry.email	NameSilo, LLC	OVH-MNT
2023-02-07T23:33:11	uswas.email	NameSilo, LLC	OVH-MNT
2023-02-07T23:33:12	crysame.email	NameSilo, LLC	OVH-MNT
2023-02-07T23:33:12	dirtyre.email	NameSilo, LLC	OVH-MNT
2023-02-07T23:33:13	badfine.email	NameSilo, LLC	OVH-MNT
2023-02-07T23:33:14	endslow.email	NameSilo, LLC	OVH-MNT
2023-02-07T23:33:15	junkan.email	NameSilo, LLC	OVH-MNT
2023-02-07T23:33:16	ithid.email	NameSilo, LLC	OVH-MNT
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"].rand(111111111,9999999999)), 0, rand(12,16)).".msi";
//$fname = "ALERT.System.Software.Upgrade.".md5($_SERVER["REMOTE_ADDR"]).".msi";
//$fname = "Antivirus.Upgrade.Database.Cloud.msi";
//$zipname = "SYSTEM.Critical.Upgrade.Win10.0.zip";
//$fname = "Antivirus_Update_Cloud.".substr(md5($_SERVER["REMOTE_ADDR"].rand(111111111,9999999999)), 0, rand(12,16)).".msi";
//$zipname = "Antivirus_Update_Cloud.".substr(md5($_SERVER["REMOTE_ADDR"].rand(111111111,9999999999)), 0, rand(12,16)).".zip";
//$fname = "SYSTEM.Antivirus.Update.".substr(md5($_SERVER["REMOTE_ADDR"].rand(111111111,9999999999)), 0, rand(12,16)).".msi";
//$zipname = "SYSTEM.Antivirus.Update.".substr(md5($_SERVER["REMOTE_ADDR"].rand(111111111,9999999999)), 0, rand(12,16)).".zip";
//$fname = "SYSTEM.Critical.Upgrade.Win10.0.".substr(md5($_SERVER["REMOTE_ADDR"].rand(111111111,9999999999)), 0, rand(12,16)).".msi";
//$zipname = "SYSTEM.Critical.Upgrade.Win10.0.".substr(md5($_SERVER["REMOTE_ADDR"].rand(111111111,9999999999)), 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

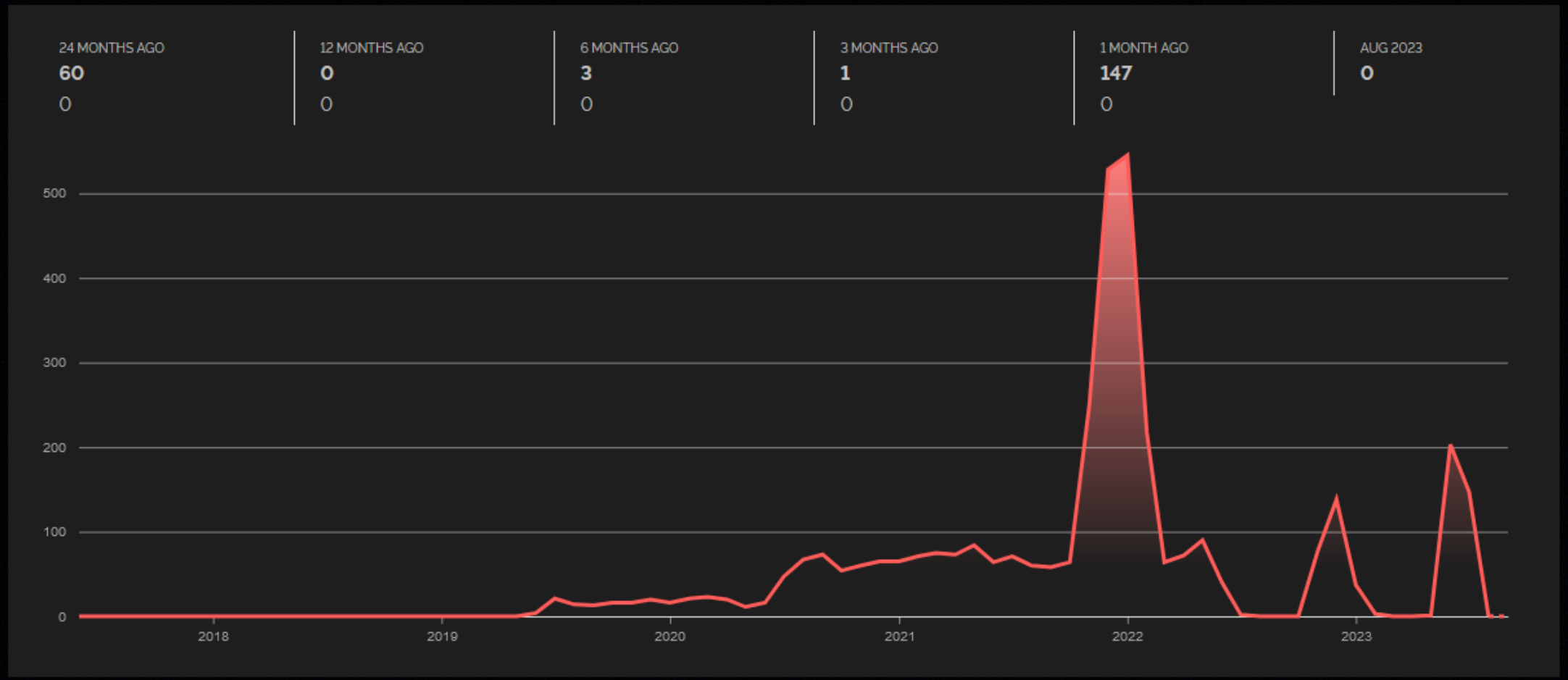
Query ➔ Timeline

Unique keyword?

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

SHODAN REMEMBERS

"NESpEp5PunEnA6a1RlO1"



DIVING INTO THE PHP SCRIPT

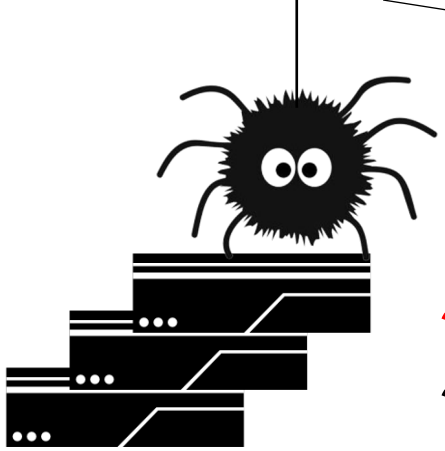
- Two hosts are excluded from anti-bot/filter checks:

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

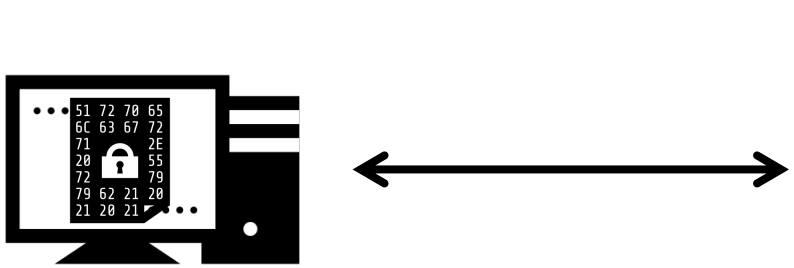
- Likely used by TA
  - Testing payloads?
  - Managing infrastructure?

- “Jump hosts”

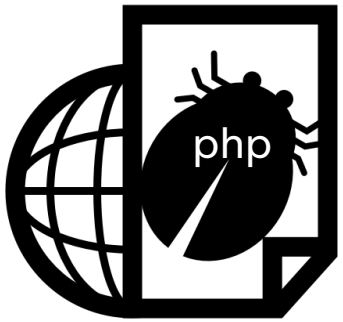
INFRASTRUCTURE



~300 hosts
~440 HTTP services



Victim

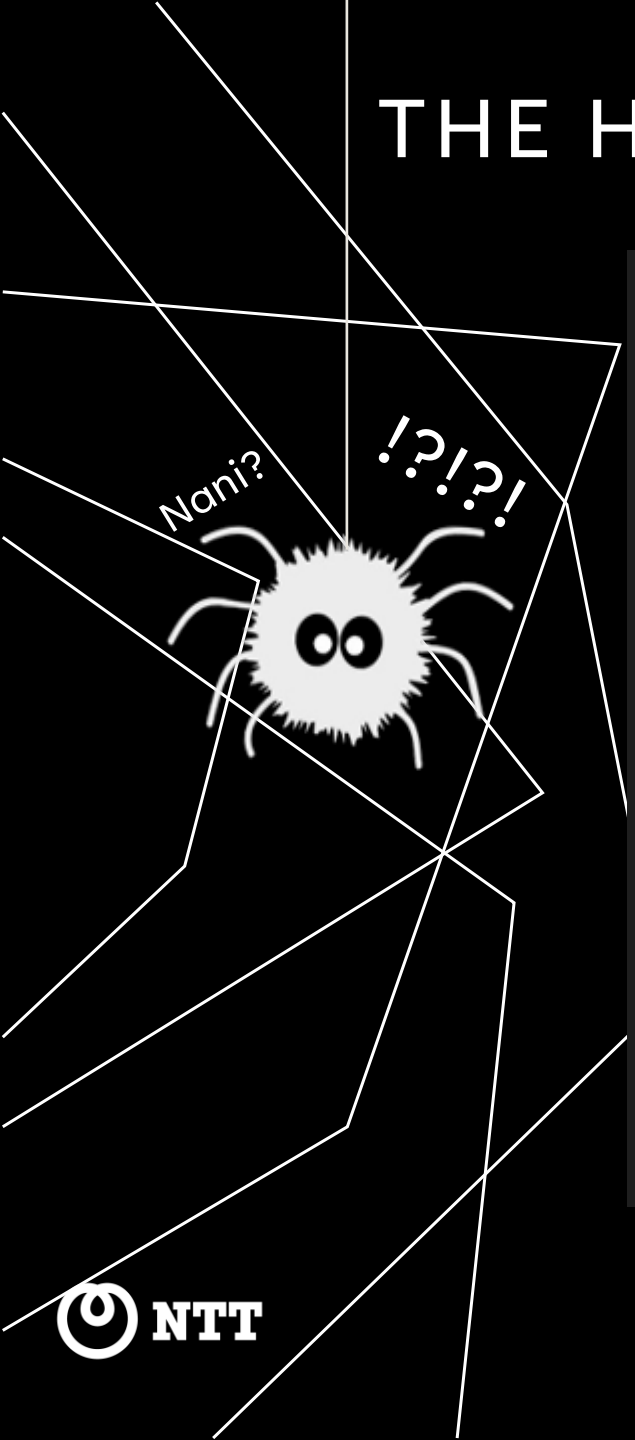


86 misconfigured servers
Payload delivery

2 jump hosts

NTT

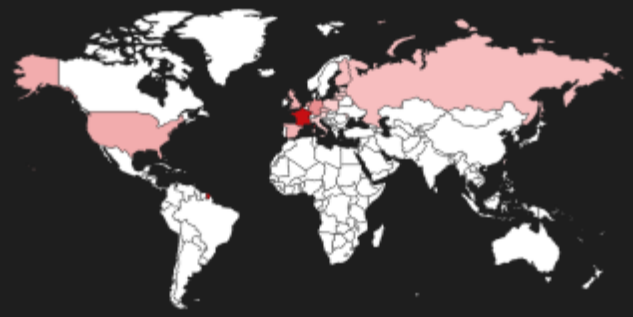
THE HUNT CONTINUE..



TOTAL RESULTS

442

TOP COUNTRIES



TOP PORTS

80	304
443	136
8080	1

Exposing log file

ohleft.site

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"

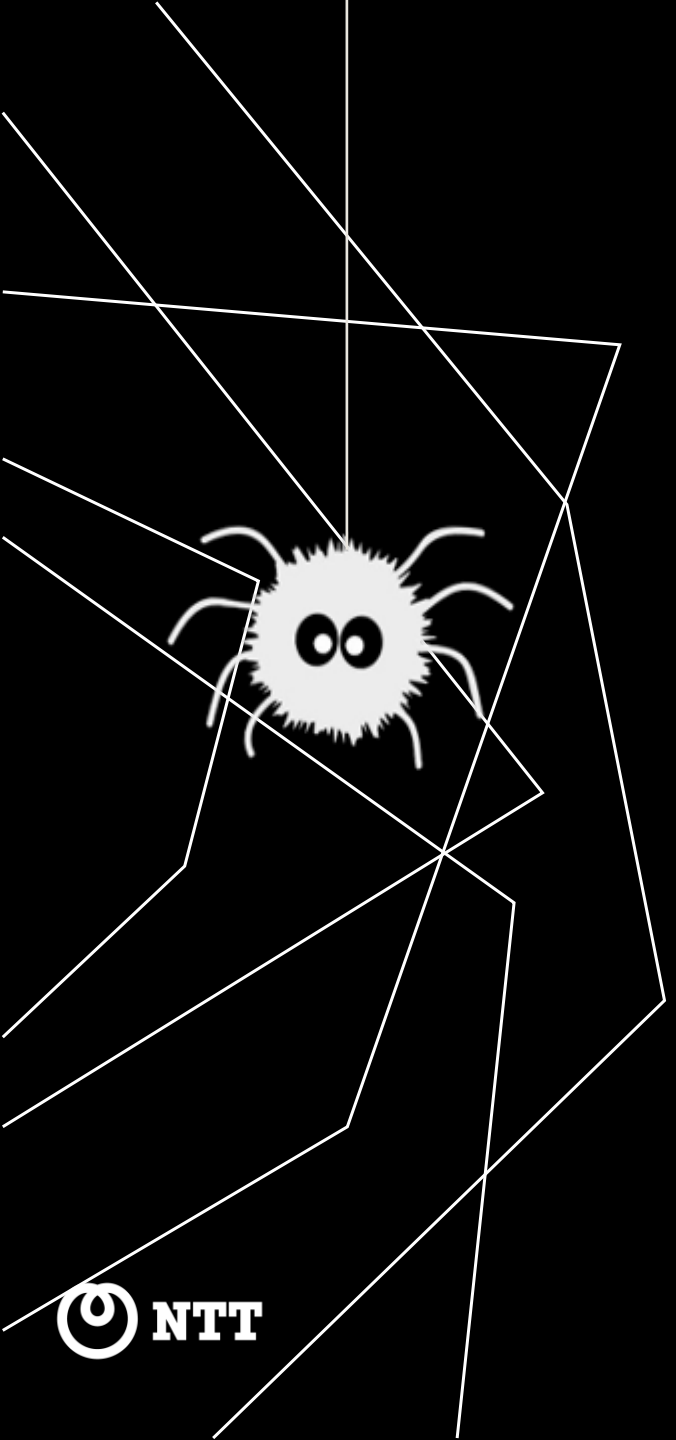
All transactions should be performed via **BITCOIN** network.

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

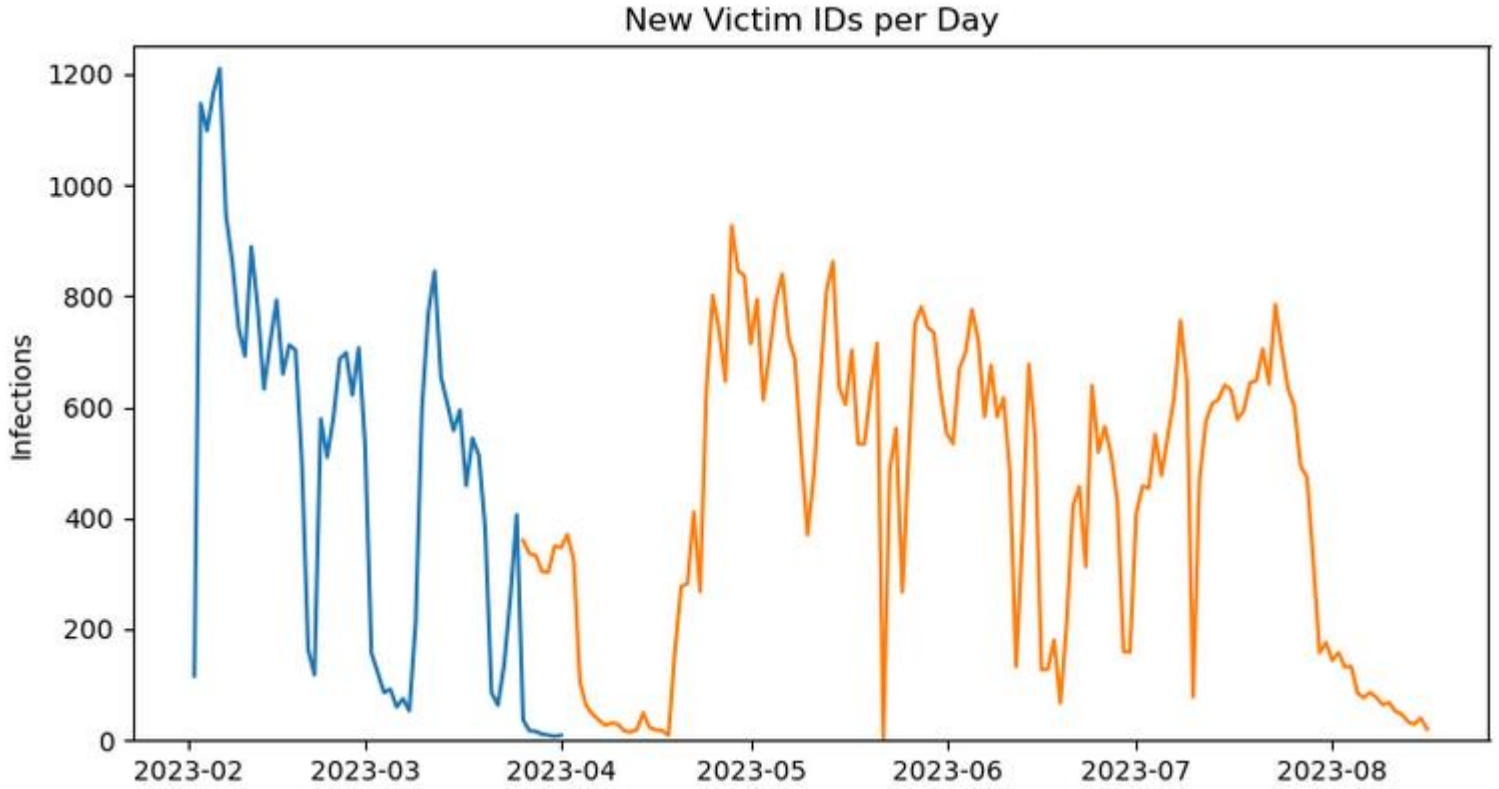
Freedecrypt:

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

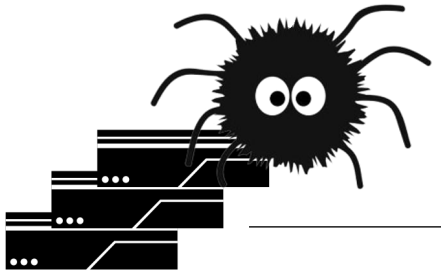
- Testing payloads

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

NTT

INFRASTRUCTURE (UPDATE)



300 Servers

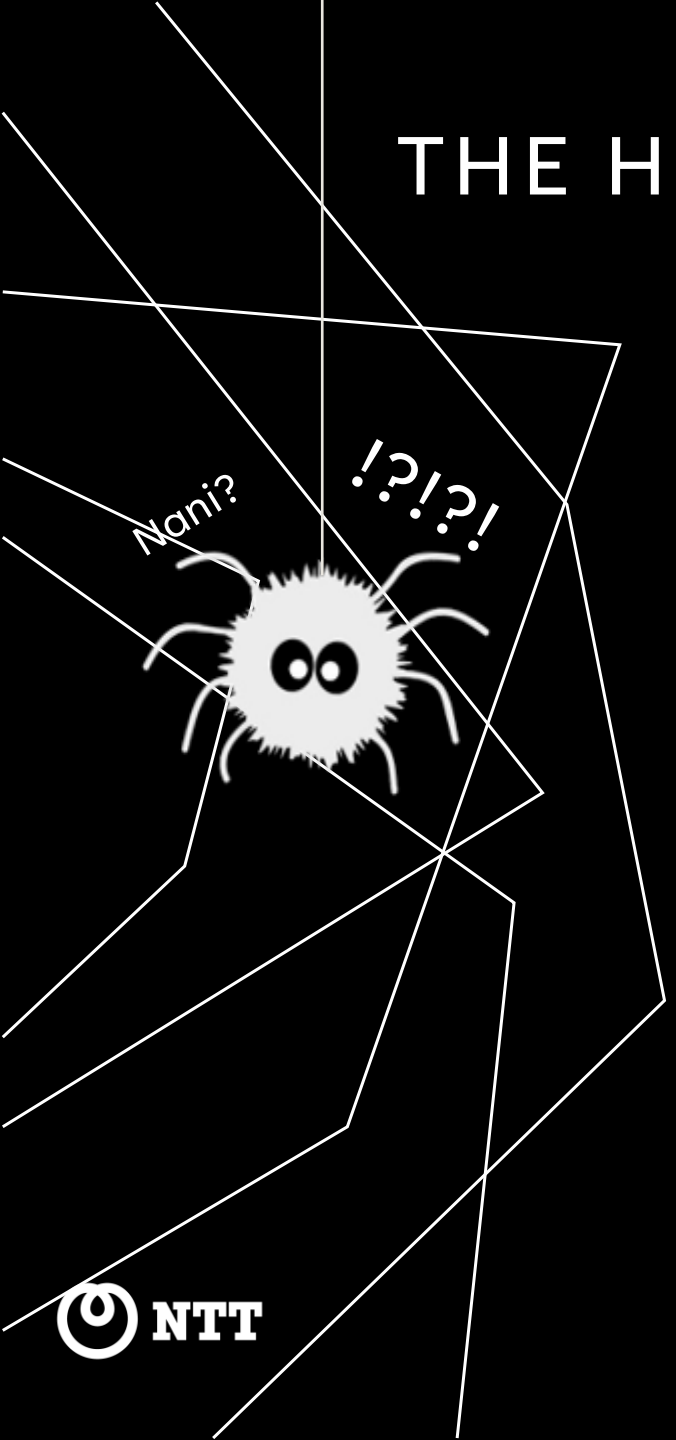
Log server:8080

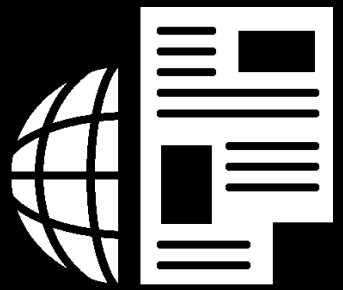
My Decryptor

Ransomware delivery

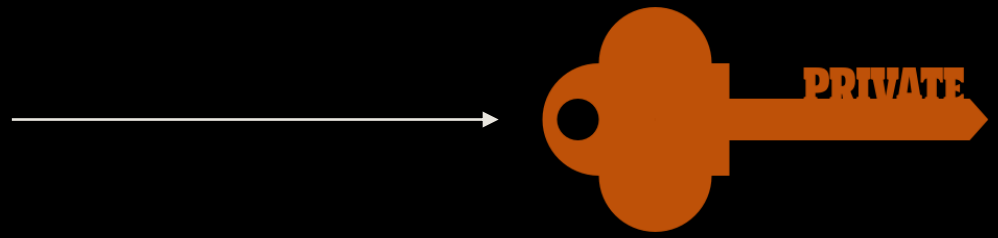
Jump host

THE HUNT CONTINUE..



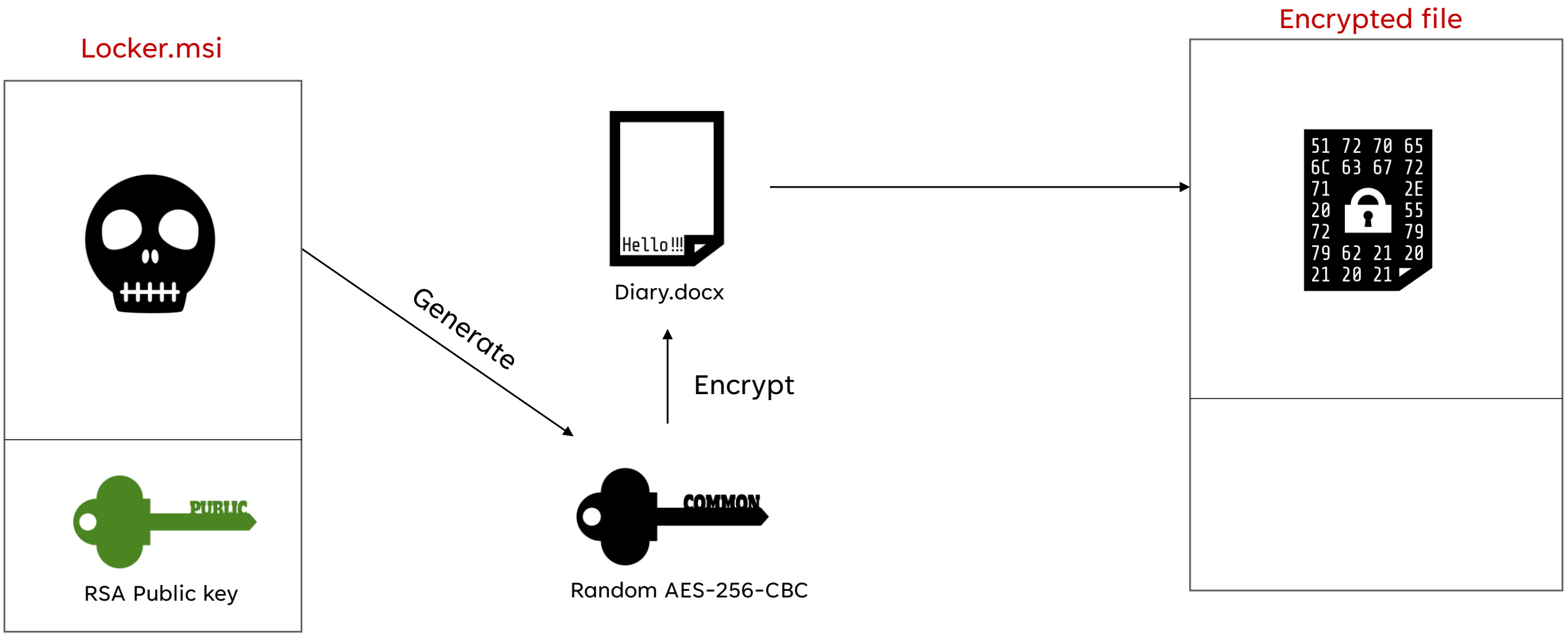


Log server:8080



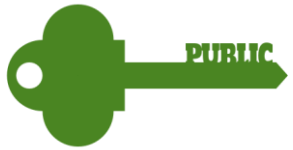
RSA Private key

MAGNIBER ENCRYPTION LOGIC



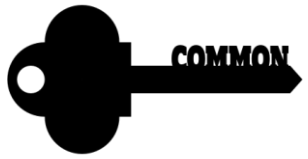
MAGNIBER ENCRYPTION LOGIC

Locker.msi



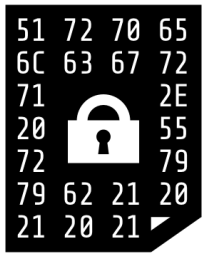
RSA Public key

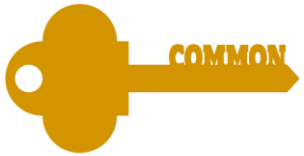
Encrypt



Random AES-256-CBC

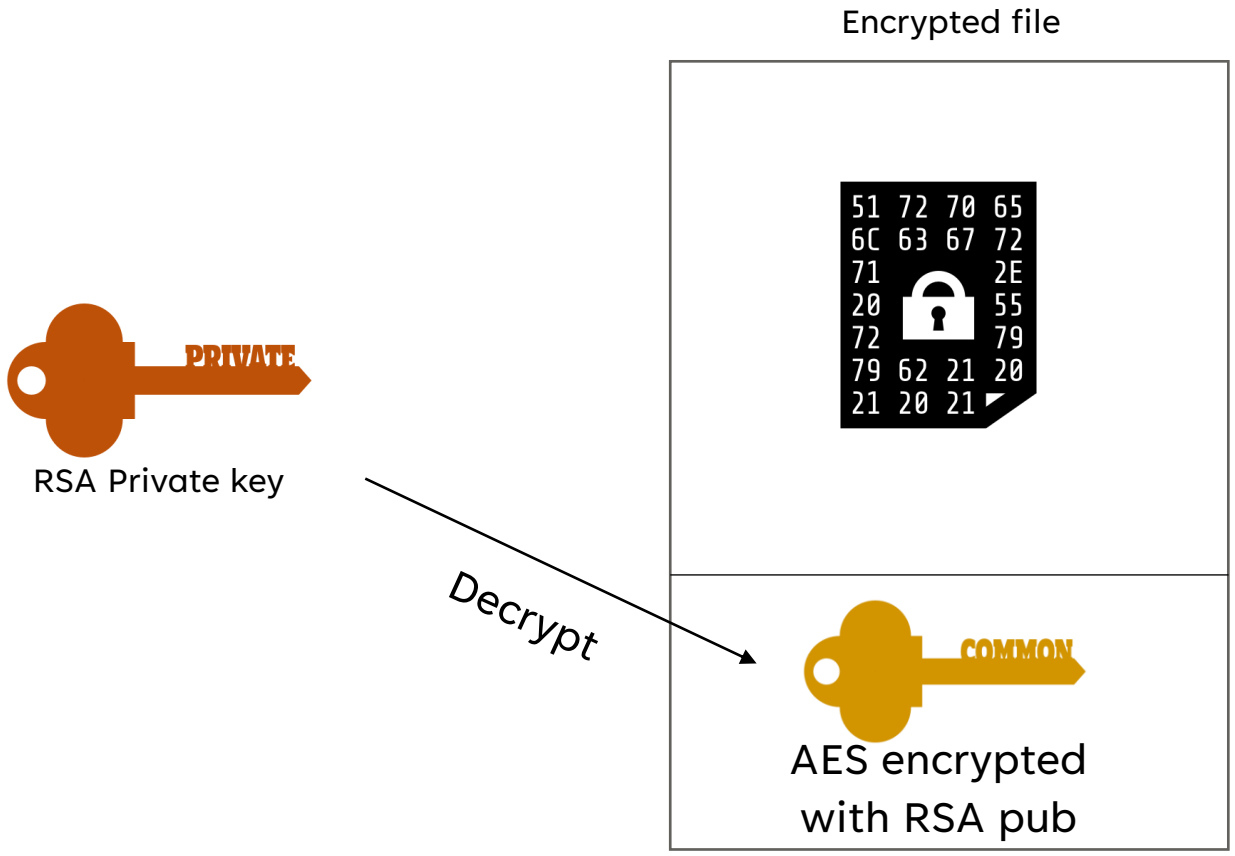
Encrypted file



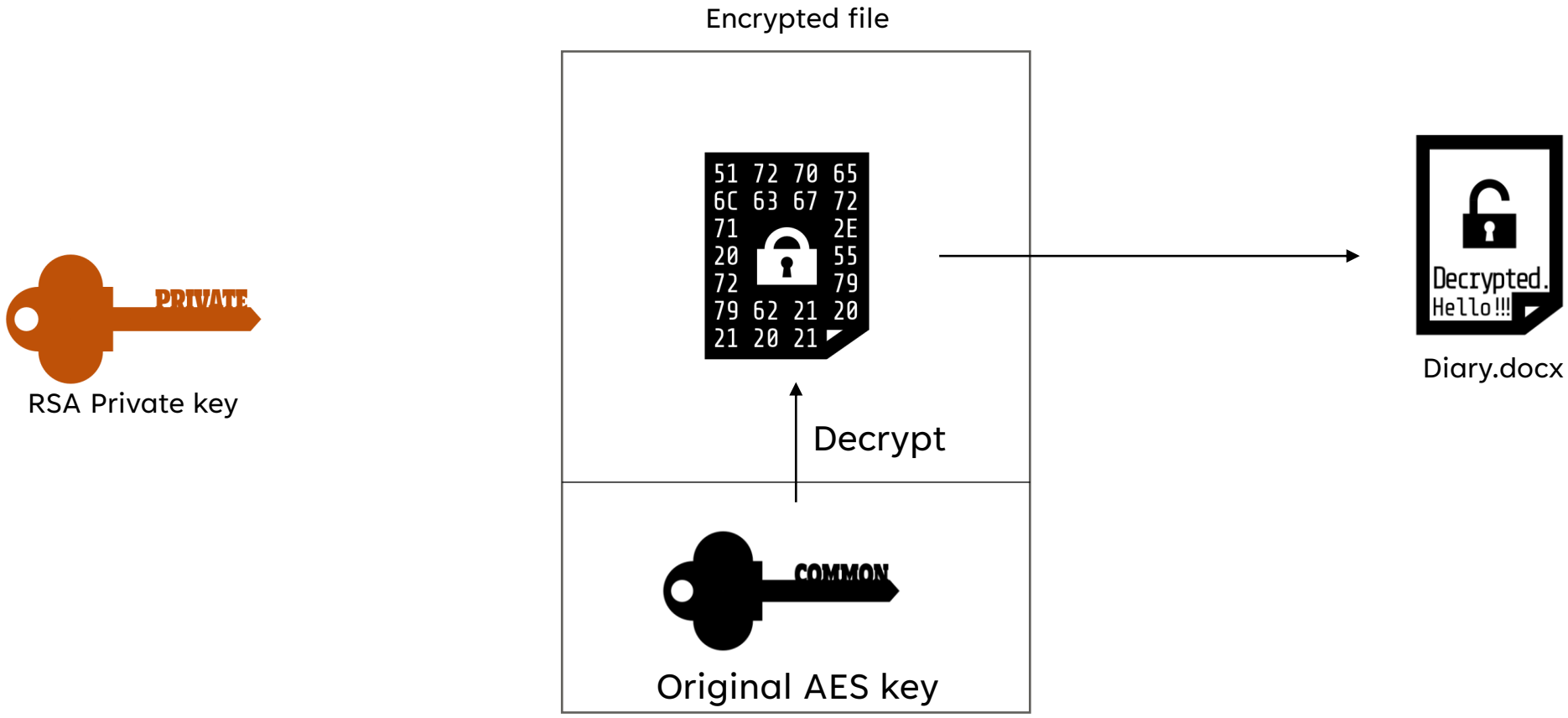


AES encrypted with RSA pub

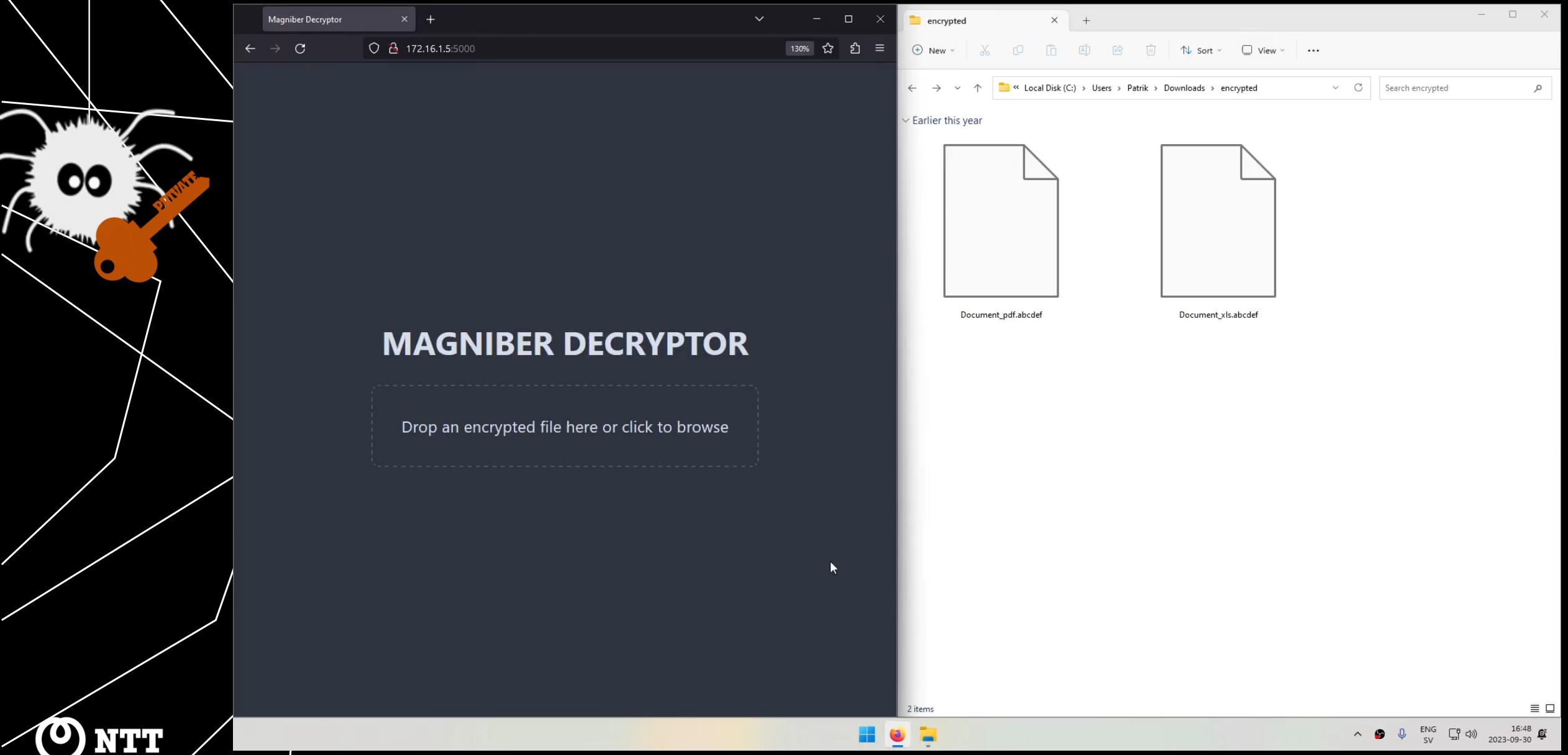
MAGNIBER DECRYPTION LOGIC

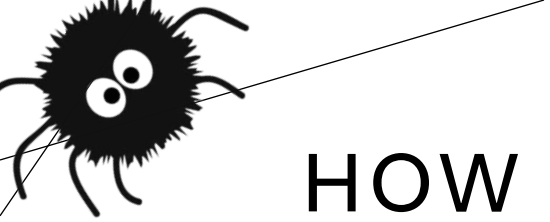


MAGNIBER DECRYPTION LOGIC



POC


Magniber Decryptor
172.16.1.5:5000
130%
MAGNIBER DECRYPTOR
Drop an encrypted file here or click to browse
encrypted
New
Sort
View
Local Disk (C:) › Users › Patrik › Downloads › encrypted
Search encrypted
Earlier this year
Document_pdf.abcdef
Document_xls.abcdef
2 items
ENG
SV
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

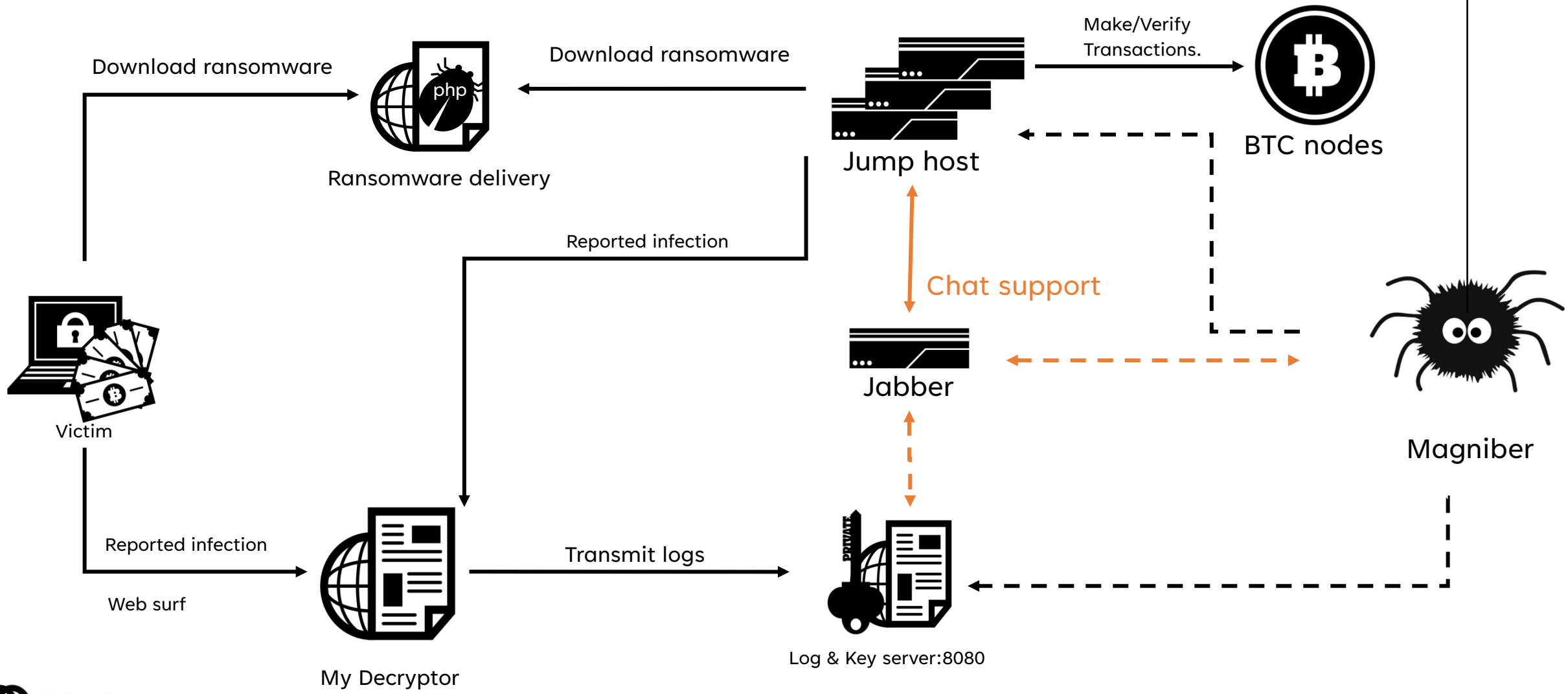
NTT


NTT
Seoul
Tokyo
Osaka
Taipei
Hong Kong
Bangkok
Kuala Lumpur
Singapore
Jakarta
Sydney
Seattle
Sacramento
Bay Area/Silicon Valley
Los Angeles
Chicago
Dallas
Houston
Boston
New York City
Washington D.C. Area
Atlanta
Miami
São Paulo
Stockholm
Amsterdam
Dusseldorf
Warsaw
London
Berlin
Brussels
Frankfurt
Vienna
Paris
Luxembourg
Munich
Budapest
Bucharest
Marseille
Milan
Sofia
Madrid
Barcelona
Valencia
TIER 1
Washington D.C. Area includes Ashburn, Reston and Dulles
Bay Area/Silicon Valley includes San Francisco, San Jose, Palo Alto and Santa Clara

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


Download ransomware
php
Ransomware delivery
Download ransomware
Jump host
Make/Verify
Transactions.
BTC nodes
Reported infection
Chat support
Jabber
Magniber
Victim
Reported infection
Web surf
My Decryptor
Transmit logs
Log & Key server:8080

SUMMARY

- Evade detection
  - DGA, 0days
- != Securing their Infra
- 89 000 victims
- 16 BTC
- https://tinyurl.com/VB2023-Magniber
  - IoCs
  - RSA keys
  - BTC addresses

NTT

Q&A

NTT

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

NTT