Navigating the Shift from Opportunistic to Targeted Ransomware Attacks

Christopher Elisan, Director of Intelligence at Flashpoint

@TOPHS
From WannaCry to LockerGoga: Navigating the Shift from Targeted to Opportunistic Ransomware Attacks

Agenda

- Introduction
- Opportunistic TTPs
- Targeted TTPs
- Why The Shift?
- Notable Differences
- Likely Targets
- Mitigation
- Questions?
Introduction

About the speaker
Christopher Elisan, Director of Intelligence at Flashpoint, is a seasoned Reverse Engineer, Malware Researcher and published Author. He speaks at conferences around the world and frequently provides expert opinion about malware, botnets and advanced persistent threats for leading industry and mainstream publications. Elisan’s published works include Hacking Exposed: Malware and Rootkits, 2 ed.

Elisan is also involved in Flashpoint’s Threat Readiness & Response (TR2) subscription, which helps companies prepare for, as well as quickly assess and respond to a ransomware or cyber extortion attack.
OPPORTUNISTIC TTPs
GandCrab Ransom Note

GandCrab Ransom Note

---END GANDCRAB KEY---
ENCRIPTED BY GANDCRAB 5.0.4

DEAR [RECIPIENT NAME],

YOUR FILES ARE UNDER STRONG PROTECTION BY OUR SOFTWARE. IN ORDER TO RESTORE IT YOU MUST BUY DECRYPTOR.

For further steps read SESDIVVZ-DECRYPT txt that is located in every encrypted folder.
GandCrab Payment Site

The payment site for GandCrab ransomware displays a countdown to double the ransom amount if the payment is not made by a specified date and time. It includes payment options for Dash and Bitcoin, with a deadline for payment.

Chat: Messages will be displayed here. Users can enter their messages and submit them for the service provider to respond.
GandCrab Panel

Dashboard

Statistics

<table>
<thead>
<tr>
<th>Date</th>
<th>Bots</th>
<th>TX</th>
<th>Orders</th>
<th>Profit</th>
<th>Fee</th>
<th>Total</th>
<th>Profit</th>
<th>Fee</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018-04-07</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>2018-04-06</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>2018-04-05</td>
<td>22</td>
<td>0</td>
<td>0</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>2018-04-04</td>
<td>49</td>
<td>0</td>
<td>1</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>2018-04-03</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>2018-04-02</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>2018-04-01</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>2018-03-31</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Total</td>
<td>72</td>
<td>0</td>
<td>1</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
</tbody>
</table>

Last transactions

<table>
<thead>
<tr>
<th>Bot</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not found</td>
<td></td>
</tr>
</tbody>
</table>
TARGETED TTPs
Ryuk Builder
Ryuk Ransom Note

Your business is at serious risk. There is a significant hole in the security system of your company. We've easily penetrated your network. You should thank the lord for being hacked by serious people not some stupid schoolboys or dangerous punks. They can damage all your important data just for fun.

Now your files are encrypted with the strongest military algorithms RSA4096 and AES-256. No one can help you to restore files without our special decoder. Photorec, RansomDecryptor etc. repair tools are useless and can destroy your files irreversibly.

If you want to restore your files write to emails (contacts are at the bottom of the sheet) and attach 2-3 encrypted files. (Less than 5 Mb each, non-archived and your files should not contain valuable information (Databases, backups, large excel sheets, etc.).

You will receive decrypted samples and our conditions how to get the decoder. Please don’t forget to write the name of your company in the subject of your e-mail.

You have to pay for decryption in Bitcoins. The final price depends on how fast you write to us. Every day of delay will cost you additional +0.3 BTC

Nothing personal just business

As soon as we get bitcoins you’ll get all your decrypted data back. Moreover you will get instructions how to close the hole in security and how to avoid such problems in the future. We will recommend you special software that makes the most problems to hackers.

Attention! One more time!

Do not rename encrypted files.
Do not try to decrypt your data using third party software.

P.S. Remember, we are not scammers. We don’t need your files and your information. But after 2 weeks all your files and keys will be deleted automatically.
Just send a request immediately after infection.
All data will be restored absolutely.
Your warranty - decrypted samples.

contact emails
elismarco@tutanota.com or
CamdenScott@protonmail.com

BTC wallet:
156LWdvm5nIn7mTvUzjg9W7w86dhyqyNj

Ryuk
No system is safe
Ryuk Process Killer

```c
new [ebp+var_88], offset aMspub_exe ; "mspub.exe"
new [ebp+var_84], offset aMydesktopops_e ; "mydesktopops.exe"
new [ebp+var_80], offset aMydesktopservice ; "mydesktopservice.exe"
new [ebp+var_7c], offset aMyqld_exe ; "mysqld.exe"
new [ebp+var_78], offset aMyqldnt_exe ; "mysqld-nt.exe"
new [ebp+var_74], offset aMyqldOpt_exe ; "mysqld-opt.exe"
new [ebp+var_70], offset aOautoupds_exe ; "oautoupds.exe"
new [ebp+var_6c], offset aOcomm_exe ; "ocomm.exe"
new [ebp+var_68], offset aOcssd_exe ; "ocssd.exe"
new [ebp+var_64], offset aOnenote_exe ; "onenote.exe"
new [ebp+var_60], offset aOracle_exe ; "oracle.exe"
new [ebp+var_5c], offset aOutlook_exe ; "outlook.exe"
new [ebp+var_58], offset aPowerpnt_exe ; "powerpnt.exe"
new [ebp+var_54], offset aSqlcoreservice ; "sqlcoreservice.exe"
new [ebp+var_50], offset aSqlagent_exe ; "sqlagent.exe"
new [ebp+var_4c], offset aSqlbrowser_exe ; "sqlbrowser.exe"
new [ebp+var_48], offset aSqlserver_exe ; "sqlserver.exe"
new [ebp+var_44], offset aSqlwriter_exe ; "sqlwriter.exe"
new [ebp+var_40], offset aSteam_exe ; "steam.exe"
new [ebp+var_3c], offset aSynctime_exe ; "synctime.exe"
new [ebp+var_38], offset aTbirdconfig_ex ; "tbirdconfig.exe"
new [ebp+var_34], offset aThebat_exe ; "thebat.exe"
new [ebp+var_30], offset aThebat64_exe ; "thebat64.exe"
new [ebp+var_2c], offset aThunderbird_exe ; "thunderbird.exe"
new [ebp+var_28], offset aWinsum_exe ; "winsum.exe"
new [ebp+var_24], offset aWinword_exe ; "winword.exe"
new [ebp+var_20], offset aWordpad_exe ; "wordpad.exe"
new [ebp+var_1c], offset aXfssuccon_exe ; "xfssuccon.exe"
new [ebp+var_18], offset aTmlisten_exe ; "tmlisten.exe"
new [ebp+var_14], offset aPccntmon_exe ; "PccNTMon.exe"
new [ebp+var_10], offset aCtaosmegr_exe ; "CNTAOsMGr.exe"
new [ebp+var_8], offset aHTmrsce_exe ; "HTmrsce.exe"
new [ebp+var_0], offset aMbantray_exe ; "mbantray.exe"
new [ebp+pe.dwSize], 22Ch
call ds:CreateToolhelp32Snapshot
new [ebp+Shapshot1], 22Ch
```
Ryuk Stopping Services
Ryuk Shadow Copy Deletion

```
File Edit Format View Help
vssadmin Delete shadows /all /quiet
vssadmin resize shadowstorage /for=c: /on=c: /maxsize=401MB
vssadmin resize shadowstorage /for=d: /on=d: /maxsize=401MB
vssadmin resize shadowstorage /for=e: /on=e: /maxsize=401MB
vssadmin resize shadowstorage /for=f: /on=f: /maxsize=401MB
vssadmin resize shadowstorage /for=g: /on=g: /maxsize=401MB
vssadmin resize shadowstorage /for=h: /on=h: /maxsize=401MB
vssadmin Delete Shadows /all /quiet
del /s /f /q c:\*.vhd c:\*.bak c:\*.wbc c:\*.bkf c:\Backup*.* c:\backup*.* c:\*.set c:\*.win c:\*.dsk
del /s /f /q d:\*.vhd d:\*.bak d:\*.wbc d:\*.bkf d:\Backup*.* d:\backup*.* d:\*.set d:\*.win d:\*.dsk
del /s /f /q e:\*.vhd e:\*.bak e:\*.wbc e:\*.bkf e:\Backup*.* e:\backup*.* e:\*.set e:\*.win e:\*.dsk
```

Likely Targets

- Organizations with deadline-driven business models, such as manufacturers and publishers. Any sort of operational disruption can result in exorbitant revenue losses for these organizations, so in the event of a ransomware attack, they are highly incentivized to restore operations as quickly as possible—even if that means paying the ransom.

- Organizations that provide critical services or infrastructure, such as healthcare, transportation, and utilities. Similar to those with deadline-driven business models, these organizations can face devastating consequences due to operational disruption and tend to be more incentivized to pay a ransom.
Why the Shift?

- Fewer victims to manage
- Bigger payday
- Discrete communication
- Less likely to have the attack campaign exposed
## Notable Differences

<table>
<thead>
<tr>
<th></th>
<th>OPPORTUNISTIC</th>
<th>TARGETED</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Infection Vectors</strong></td>
<td>Spam, Watering hole</td>
<td>Spear Phishing, RDP, Vulnerability, Stolen Creds, Partner Compromise</td>
</tr>
<tr>
<td><strong>Ransomware Behavior</strong></td>
<td>Targets user services, protection services</td>
<td>Targeting Server software</td>
</tr>
<tr>
<td><strong>Ransom Comms</strong></td>
<td>TOR site</td>
<td>Email</td>
</tr>
<tr>
<td><strong>Ransom $</strong></td>
<td>Up to $3000</td>
<td>Upwards to millions of $</td>
</tr>
</tbody>
</table>
To protect yourself from future infections:
1) Set a security protocol so that your employees do not open any attachments from unverified sources.
2) Secure email gateways to thwart threats via spam and avoid opening suspicious emails. Set up your workstations to not automatically open scripts and attached files.
3) Keep AntiViruses updated and only centrally controlled preferably on web console, with its own separate credentials rather than Domain Administrators.
4) Enforce the principle of least privilege: Secure system administrations tools that attackers could abuse; implement network segmentation and data categorization to minimize further exposure of mission-critical and sensitive data; disable third-party or outdated components that could be used as entry points.
5) Keep systems and applications updated, or use virtual patching for legacy or unpatchable systems and software.
6) When you have restored all your files change all passwords.
7) Use different passwords for local administrators on each computer.
Protection & Mitigation

- Regular, organized backups, separate from network
- Dual-factor authentication
- Encryption of sensitive data
- RDP access facing the Internet - disable or patch
- Email and Social Media security/training
- Ransomware prevention tools designed to monitor files and folders for changes and stop encryption processes
  - RansomFree
  - Bitdefender's Anti-Ransomware Tool
  - Cryptostalker
- CryptoSearch, a tool that automates the process for finding files encrypted by ransomware. This allows for the storing of encrypted files until a decryption solution is available.
THANK YOU!

STAY CONNECTED:
HTTPS://WWW.FLASHPOINT-INTEL.COM

TWITTER:
@FLASHPOINTINTEL