The Evolution of GandCrab Ransomware

Tamas Boczan
@tamas_boczan
Sr. Threat Analyst
Why?
Why?
Business Model: RaaS
Mass Delivery Methods

- Email attachments
  - Javascript
  - Doc
  - Encrypted doc
- Drive-by download
Delivery: RDP, Exploits

**TOTAL RESULTS**

2,558,684

**TOP COUNTRIES**

- China: 674,703
- United States: 542,059
- Germany: 114,138
- Brazil: 112,129
- Russian Federation: 72,462

**TOP SERVICES**

- RDP: 2,524,117
- RDP (3388): 33,904
- CMD: 44

---

140.120.31.200

**Remote Desktop Protocol**

Added on 2018-11-10 20:15:08 GMT

Taiwan, Taichung

Details

132.232.22.150

**Tencent cloud computing**

Added on 2018-11-10 20:12:05 GMT

China

Details

- **SSL Certificate**
  - Issued By:
  - Common Name:
  - Issued To:
  - Common Name:
- **Supported SSL Versions**
  - TLSv1, TLSv1.1, TLSv1.2
- **Diffie-Hellman Parameters**
  - Fingerprint: RFC2409/Oakley Group 2

18.222.229.92
Payload: Starting Point

Data collection

- System Info
- External IP
- AV?
Data collection
- System Info
- External IP
- AV?

Connect Home
- nslookup
Payload: Starting Point

Data collection
- System Info
- External IP
- AV?

Connect Home
- nslookup

Preparation
- Kill Processes
Payload: Starting Point

Data collection
- System Info
- External IP
- AV?

Connect Home
- nslookup

Preparation
- Kill Processes

Encryption
- AES
- *.GDCB
Payload: Starting Point

Data collection
- System Info
- External IP
- AV?

Connect Home
- nslookup

Preparation
- Kill Processes

Encryption
- AES
- *.GDCB

Post-Infection
- Shadow Copies
Feb 28: Europol decryptor

- **Data collection**
  - System Info
  - External IP
  - AV?

- **Connect Home**
  - nslookup

- **Preparation**
  - Kill Processes

- **Encryption**
  - AES
  - *.GDCB

- **Post-Infection**
  - Shadow Copies
7 days later: v2

Data collection
- System Info
- External IP
- AV?
  - Kernel-AV

Connect Home
- nslookup

Preparation
- Kill Processes

Encryption
- AES
- *.CRAB

Post-Infection
- Shadow Copies
7 weeks later: v3

Post-Infection

- Shadow Copies
- Wallpaper
Data collection
- System Info
- External IP
- AV?

Connect Home
- nslookup

Preparation
- Kill Processes

Encryption
- AES
- Salsa
- *.KRAB
- SMB shares

Post-Infection
- Shadow Copies
- Wallpaper
- Self-removal
Data collection
- System Info
- AV?

Connect Home
- WPress hacks
- URL generation

Preparation
- Kill Processes

Encryption
- Salsa
- *.KRAB
- SMB shares

Post-Infection
- Shadow Copies
- Wallpaper
- Self-removal
Vaccine: Jul 13
Zero day details

- BSOD, no RCE
- Full disclosure, not used
- Why?
  - Retaliation
  - Overestimated impact
- Probably just fuzzed it
Data collection
- System Info
- AV?

Connect Home
- WPress hacks
- URL generation

Preparation
- Kill Processes
- Escalate

Encryption
- Salsa
- `.Random`
- SMB shares

Post-Infection
- Shadow Copies
- Wallpaper
- Self-removal
v5: Maintenance

**Data collection**
- System Info
- AV?

**Connect Home**
- WPress hacks
- URL generation

**Preparation**
- Kill Processes
- Escalate

**Encryption**
- Salsa
- *.Random
- SMB shares

**Post-Infection**
- Shadow Copies
- Wallpaper
- Self-removal
Retired?

Gandcrab

We are leaving for a well-deserved retirement.

We personally earned more than 150 million dollars per year.

For the year of working with us, people have earned more than $2 billion.
What We Learned: Developer’s Profile

- > RaaS marketing skills
- Project organization:
  > react quickly
  < poor quality
- Exploit development capability:
  > implement exploits based on POCs
  > find simple exploit via fuzzing
  < can’t develop more complex RCE exploit
  < can’t guess impact of an exploit
The Evolution of GandCrab Ransomware

Tamas Boczan
@tamas_boczan
Sr. Threat Analyst