REMOTE ACCESS TOOLS

The Hidden Threats Inside Your Network

SANS THIR 2019
Agenda

- Why care about RATs?
- RAT detection today
- A better way forward
- Findings from the field
- Digging into the weeds
Why care about RATs?

RAT Ratatouille: Backdooring PCs with leaked RATs

Canadian Police Raid ‘Orcus RAT’ Author

Canadian police last week raided the residence of a Toronto software developer behind “Orcus RAT,” a product that’s been marketed on underground forums and used in countless malware attacks since its creation in 2015. Its author maintains Orcus is a
RATs leak the darndest things...

**Device serial number**

**MAC address and OS**

**My public AND private IP addresses and ports**

**TeamViewer**
- Magic: 0x1130 command2
- Command: CMD_UDPFLOWCONTROL (97)
- Length: 156
- Header packet ID: 20
- Header request ID: 23
- Header command class: 27
- Header offset: 24
- Data Captured: \003

**UDP**
- Destination IP: 3.58.220
- Destination Port: 52242
- Private Destination Port: 52242

**Encrypted Application Data:**
- 4a45444920476d726571756573743d70696e67266a6564693d31...
RAT detection today

• Discover
  • Find the RATs you care about
  • Identify their indicators (DNS, IPs, domains, etc…)

• Take Action
  • Capture all of this in $SECURITY TOOL

• Hope…
  • No changes occur to the infrastructure
  • No other RATs become important

Remind you of anything?
**RAT detection today**

- **Discover**
  - Find the RATs you care about
  - Identify their indicators (DNS, IPs, domains, etc.)

- **Take Action**
  - Capture all of this in $SECURITY_TOOL$

- **Hope**
  - No changes occur to the infrastructure
  - No other RATs become important

Remind you of anything?

Image: https://www.performanceicreate.com
A better way forward
Isn’t that neat?

You can tell it's an Aspen Tree because of the way it is. How neat is that?

5:02 PM - 24 Mar 2013

https://www.youtube.com/watch?v=6jgvNqNKJ5Q&feature=youtu.be
Back to Basics: Identify important RAT capabilities

Severity if accomplished by adversary

- Remote Control
- File Upload
- File Download
- Remote View
- Remote Audio
B2B: Identify likely behaviors of capabilities

Session Duration

- Remote Control, View, or Audio are most effective over long-lived sessions (i.e. minutes)
B2B: Identify likely behaviors of capabilities

Session Duration

• Remote Control, View, or Audio are most effective over long-lived sessions (i.e. minutes)
• File transfer session durations are dependent on size and throughput
B2B: Identify likely behaviors of capabilities

Packet Characteristics

- File uploads have:
  - large source packets
  - small destination packets
  - high sent to received packets ratio (outflow of data)
B2B: Identify likely behaviors of capabilities

Packet Characteristics

• File uploads have:
  • large source packets
  • small destination packets
  • high sent to received packets ratio (outflow of data)

• File downloads have:
  • large destination packets
  • small source packets
  • low sent to received packets ratio (inflow of data)
B2B: Identify likely behaviors of capabilities

Packet Characteristics

• File uploads have:
  • large source packets
  • small destination packets
  • high sent to received packets ratio (outflow of data)

• File downloads have:
  • large destination packets
  • small source packets
  • low sent to received packets ratio (inflow of data)

• Remote audio has:
  • small packets (lag is bad!)
B2B: Identify likely behaviors of capabilities

Data Reliability

• File transfers must be highly-reliable
B2B: Identify likely behaviors of capabilities

Data Reliability

- File transfers **must** be highly-reliable
- Remote Control, View, or Audio can tolerate missing data
B2B: Identify likely behaviors of capabilities

Transport-Layer Protocol

- File transfers use TCP
  - Sometimes HTTP or TLS, other times tunneled
B2B: Identify likely behaviors of capabilities

Transport-Layer Protocol

- File transfers use TCP
  - Sometimes HTTP or TLS, other times tunneled
- Remote Control, View, or Audio use either TCP or UDP
Visualizing behaviors

• Remote GUI via Quasar
Visualizing behaviors

- Exfil via RDP
Visualizing behaviors

- Infil via LogMeIn (small file)
Putting it all together

<table>
<thead>
<tr>
<th>Capability</th>
<th>Session Duration</th>
<th>Packet Characteristics</th>
<th>Data Reliability</th>
<th>Transport-Layer Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Control</td>
<td>Long-lived</td>
<td>Large source</td>
<td>Must-have</td>
<td>Something on top of TCP</td>
</tr>
<tr>
<td>File Upload</td>
<td>Depends</td>
<td>Small source</td>
<td>Nice-to-have</td>
<td>Anything goes</td>
</tr>
<tr>
<td>File Download</td>
<td></td>
<td>Large destination</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote View</td>
<td></td>
<td>Small destination</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote Audio</td>
<td></td>
<td>Data inflow</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data outflow</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
What about the destination?

• Is it common in your network?
What about the destination?

• Is it common in your network?
• Is it named?
What about the destination?

- Is it common in your network?
- Is it named?
- Is it owned by a business? Is it a home IP?
What about the destination?

• Is it common in your network?
• Is it named?
• Is it owned by a business? Is it a home IP?
• Is it associated with TOR? VPS? Public Cloud?
What about the destination?

• Is it common in your network?
• Is it named?
• Is it owned by a business? Is it a home IP?
• Is it associated with TOR? VPS? Public Cloud?
• Is there any OSINT about it?
Why behavior-based?

<table>
<thead>
<tr>
<th>Traditional Technique</th>
<th>Adversary Evasion</th>
<th>Difficulty for Adversary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain identification</td>
<td>Register new domain</td>
<td>Easy</td>
</tr>
<tr>
<td>IP/Range identification</td>
<td>Use new provider</td>
<td>Easy</td>
</tr>
<tr>
<td>String match</td>
<td>Change string</td>
<td>Easy</td>
</tr>
</tbody>
</table>
## Why behavior-based?

<table>
<thead>
<tr>
<th>Traditional Technique</th>
<th>Adversary Evasion</th>
<th>Difficulty for Adversary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain identification</td>
<td>Register new domain</td>
<td>Easy</td>
</tr>
<tr>
<td>IP/Range identification</td>
<td>Use new provider</td>
<td>Easy</td>
</tr>
<tr>
<td>String match</td>
<td>Change string</td>
<td>Easy</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Behavioral Technique</th>
<th>Adversary Evasion</th>
<th>Difficulty for Adversary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify File Upload/Download behavior</td>
<td>Rewrite file transfer mechanism</td>
<td>Hard</td>
</tr>
<tr>
<td>Identify long-lived session behavior</td>
<td>Rewrite communication mechanism</td>
<td>Hard, Disruptive</td>
</tr>
</tbody>
</table>
Findings from the field

- RDP (TCP and UDP)
- TeamViewer (TCP and UDP)
  - session 74 hours in length!
- Remote access to lab infrastructure tunneled over SSH (TCP)
- WinSCP file transfer (TCP)
- WebEx, Zoom, Slack video (UDP)
Digging into the weeds on your own

<table>
<thead>
<tr>
<th>Tool</th>
<th>Best Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireshark</td>
<td>in-depth analysis</td>
</tr>
<tr>
<td>CyberChef</td>
<td>rapid prototyping</td>
</tr>
<tr>
<td>Lua</td>
<td>reusable parsers</td>
</tr>
</tbody>
</table>
## Digging into the weeds on your own

<table>
<thead>
<tr>
<th>Tool</th>
<th>Best Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireshark</td>
<td>in-depth analysis</td>
</tr>
<tr>
<td>CyberChef</td>
<td>rapid prototyping</td>
</tr>
<tr>
<td>Lua</td>
<td>reusable parsers</td>
</tr>
</tbody>
</table>

LogMeIn and TeamViewer blog posts

DEF CON 26 workshop on protocol analysis via RE

Optiv’s TeamViewer blog series
Questions?

Email: david@awakesecurity.com
Twitter: @davidp0508
LinkedIn
Awake Blog

Thank You!