To Catch a Ratter: Monitoring the Behavior of Amateur DarkComet RAT Operators in the Wild

Brown Farinholt, Haikuo Yin, Kirill Levchenko
Mohammad Rezaeirad
Paul Pearce
Hitesh Dharmdasani
Stevens Le Blond
Damon McCoy

UC San Diego
George Mason University
UC Berkeley
Informant Networks
EPFL & MPI-SWS
New York University

Credit: https://2.bp.blogspot.com/-AEfsciiO6ig/UzmUYteaQ8I/AAAAAAAAa7o/pQTAm5m0rjw/s1600/Remote-access-Trojan-njRAT.jpg
Remote Access Trojans

• Let attackers control infected machines remotely
• Do not have exploits
• Operated **manually** vs. scripted malware
  • Ransomware, botnets are automated
  • RAT infections controlled by **human operator**
Capabilities

- Webcam & Microphone
- Chat Client
- Remote Desktop
- Filesystem
- Passwords & Keylogger
- Network Interrogation & Attack
Low Barrier to Entry

Availability: YouTube

Community: Dedicated Hacking Forums

How to setup Dark Comet RAT (with download and pictures): hacking
https://www.reddit.com/r/hacking/how_to_setup_dark_comet_rat_with_download_and/

How to Download and Use DarkComet 5.3.1 - YouTube
https://www.youtube.com/watch?v=VYoYknY6oOw
Mar 12, 2013 - Uploaded by Knihtztle
LINKS: DarkComet 5.3.1: http://www.mediafire.com/?emnqkegq71745o
Sandboxie: http://www.sandboxie.com...

How to Download and Use DarkComet 5.3.1 [2016 updated] - YouTube
https://www.youtube.com/watch?v=585SMF0nNYs
Feb 11, 2016 - Uploaded by No Name
UPDATED 2016-10-08 DarkComet 5.3.1: http://www.mediafire.com/file/54a3qmpthc78wcy/5DarkComet_5.3.1...

How To Setup DarkComet R.A.T Be Successful With It - YouTube
https://www.youtube.com/watch?v=7t8_dqGs6EL
Nov 2, 2015 - Uploaded by imSoSittingBANNED
its clean ... let me know when all the links eventually go down. DarkComet: https:...image.nzb6ke6c3i.QB

Setup a DarkComet RAT correctly [Tutorial] [Download] [No-IP] [2015 ...
https://www.youtube.com/watch?v=REWvF9S9P5g
Feb 17, 2015 - Uploaded by Prehocks
Download: http://astf/ry13306x FUD Credient: https://www.youtube.com/watch?v=m1bA0USvJUt0C Open ...
Widespread Usage
Voyeurism

• School-issued laptop webcams

• Black market for webcam access
Widespread Usage

**Voyeurism**

- School-issued laptop webcams
- Black market for webcam access

**Sextortion & Blackmail**

- *Black Mirror*: “Shut Up and Dance”
- Miss Teen USA
Widespread Usage

Voyeurism

- School-issued laptop webcams
- Black market for webcam access

Sextortion & Blackmail

- *Black Mirror*: “Shut Up and Dance”
- Miss Teen USA

Surveillance & Espionage

- Syria DarkComet Skype tool
Widespread Usage

Voyeurism
- School-issued laptop webcams
- Black market for webcam access

Sextortion & Blackmail
- *Black Mirror*: “Shut Up and Dance”
- Miss Teen USA

Surveillance & Espionage
- Syria DarkComet Skype tool

- Attacks can be targeted...
- But many attackers seek large numbers of victims
  - Spread online (download links, cracked software)

Common Theme:
Accessing victim user
Research Questions & Motivation
Research Questions & Motivation

What do RAT operators do with compromised machines?
What do RAT operators do with compromised machines?

Goal: To understand common use patterns of RATs in the wild (at scale)

- RATs used criminally, cause harm
- Elicit attacker methods, motivations
- Evaluate potential defenses
- Generally understand their use cases
The Plan
The Plan

- Acquired **DarkComet RAT samples** from VirusTotal
The Plan

- Acquired *DarkComet RAT samples* from VirusTotal
- Executed them in malware sandbox *honeypots*
The Plan

- Acquired **DarkComet RAT samples** from VirusTotal
- Executed them in malware sandbox **honeypots**
- Recorded **network traces** of operator interaction
The Plan

- Acquired **DarkComet RAT samples** from VirusTotal
- Executed them in malware sandbox **honeypots**
- Recorded **network traces** of operator interaction
- Decrypted to obtain **operator command** sequences
Experiment
Experiment

19,109 samples
Experiment

- 19,109 samples
- 13,339 addresses
Experiment

- 19,109 samples
- 13,339 addresses
- 9,877 operators

- 89% residential IPs
- 37% Turkish (#1)
- 15% Russian (#2)
- Diurnal liveness pattern
Experiment

19,109 samples

13,339 addresses

9,877 operators
Experiment

19,109 samples → 13,339 addresses → 9,877 operators

1,165 live samples
Experiment

19,109 samples

13,339 addresses
1,165 live samples
19,109 samples
9,877 controllers
Experiment

19,109 samples

13,339 addresses
1,165 live samples
19,109 samples
9,877 controllers

Applications
Experiment

[Image of a computer screen showing various applications and a filesystem window.]

- **19,109 samples**
  - Applications
  - Filesystem
Experiment

19,109 samples

13,339 addresses
1,165 live samples
19,109 samples
9,877 controllers

Applications

Filesystem

Browser History

Honey-Credentials
Experiment

19,109 samples → 13,339 addresses → 9,877 operators

1,165 live samples
Experiment

19,109 samples
13,339 addresses
1,165 live samples
9,877 operators
777 interactions
4 Weeks
Experiment

19,109 samples

13,339 addresses

9,877 operators

1,165 live samples

777 interactions

4 Weeks
Experimental Biases
Targeted Attacks

We do not emulate specific targets.
Targeted Attacks

We do not emulate specific targets.

DarkComet

DarkComet is a favorite of script kiddies.
Experimental Biases

**Targeted Attacks**

We do *not* emulate specific targets.

**DarkComet**

DarkComet is a favorite of script kiddies.

**Infection Longevity**

One hour time limit prevents return.
Experimental Biases

Targeted Attacks

We do *not* emulate specific targets.

DarkComet

DarkComet is a favorite of script kiddies.

Infection Longevity

One hour time limit prevents return.

Honeypot Limitations

- No webcam or microphone feeds
- No responses to attacker-initiated chat, communication
- No keystrokes for keylogger
- Virtual machine indicators
- Network containment policy
Common Patterns of Action

777 sessions
Common Patterns of Action

- Webcam, Audio

777 sessions

First Action: 31%
Second Action: 13%
Third Action: 8%

Last Action: ...
(Attempted) User Monitoring

Spy Functions
- Webcam Capture
- Sound Capture
- Remote Desktop
- Keylogger
(Attempted) User Monitoring

Webcam: 61%
(Attempted) User Monitoring

Webcam: 61%

Microphone: 26%
(Attempted) User Monitoring

Webcam: 61%  Microphone: 26%

• Recall: We do not provide webcam / microphone feeds
• Motivation unknown!
Webcam, Audio

Common Patterns of Action

First Action: 31%
Second Action: 13%
Third Action: 8%

777 sessions
Common Patterns of Action

777 sessions

First Action: 31%
Second Action: 13%
Third Action: 8%
Last Action: 19%

Webcam, Audio (31%)
Passwords (11%)
Credential Theft

- Passwords / Datas
  - Stored Passwords
    - uTorrent Downloads

- Spy Functions
  - Webcam Capture
  - Sound Capture
  - Remote Desktop
  - Keylogger
Credential Theft

Passwords: 43%

- Credentials seeded on honeypots were used 13 times outside study
- **Steam** (gaming platform) was probed often
Credential Theft

Passwords: 43%

Keylogger: 31%

- Credentials seeded on honeypots were used 13 times outside study
- **Steam** (gaming platform) was probed often
- For one-click actions, these numbers are low… Recreational users?
Common Patterns of Action

- **Webcam, Audio**
  - First Action: 31%
  - Second Action: 13%
  - Third Action: 8%
  - Last Action: 19%

- **Passwords**
  - First Action: 11%
  - Second Action: 7%
  - Third Action: 6%
  - Last Action: 8%

777 sessions
Common Patterns of Action

- First Action: 31% (Filesystem)
- Second Action: 13% (Password)
- Third Action: 8% (Password)
- Last Action: 19% (Webcam, Audio)

777 sessions
Filesystem Access
Filesystem Access

Filesystem Exploration: **40%**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>C:</td>
<td>Folder</td>
<td></td>
</tr>
<tr>
<td>D:</td>
<td>Folder</td>
<td></td>
</tr>
<tr>
<td>Z:</td>
<td>Folder</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>..</td>
<td>Folder</td>
</tr>
<tr>
<td>DCSCMIN</td>
<td>Folder</td>
</tr>
<tr>
<td>My Games</td>
<td>Folder</td>
</tr>
<tr>
<td>My Music</td>
<td>Folder</td>
</tr>
<tr>
<td>My Pictures</td>
<td>Folder</td>
</tr>
</tbody>
</table>
Filesystem Access

- 4% of attackers uploaded hacking tools
- 34 unique executables uploaded, 19 new to VirusTotal
Filesystem Access

- 4% of attackers uploaded hacking tools
- 34 unique executables uploaded, 19 new to VirusTotal
- Bitcoin wallets, Steam configs downloaded often
Common Patterns of Action

First Action
- Web: 31%  
- Passwords: 11%
- Webcam, Audio: 7%
- Filesystem: 6%
- Other: 19%

Second Action
- Web: 13%  
- Passwords: 7%
- Webcam, Audio: 7%
- Filesystem: 7%
- Other: 12%

Third Action
- Web: 8%  
- Passwords: 6%
- Webcam, Audio: 7%
- Filesystem: 7%
- Other: 19%

Last Action
- Web: 7%  
- Passwords: 7%
- Webcam, Audio: 7%
- Filesystem: 7%
- Other: 12%

777 sessions
Common Patterns of Action

- First Action: 31%
- Second Action: 13%
- Third Action: 8%
- Last Action: 19%

- Remote Desktop: 30%
- Filesystem: 24%
- Passwords: 21%
- Webcam, Audio: 17%

777 sessions
Remote Desktop

Remote Desktop: 83% !
Remote Desktop

Remote Desktop: 83%!

**Active RD:** 56%

- GUI-based hacking tools
- Applications (Steam, browsers)
Remote Desktop

Havij SQL Injector

Havij - Advanced SQL Injection Tool

Version 1.10 Pro
Copyright © 2009-2012
By r3dm0v3

http://ITSecTeam.com
http://forum.ITSecTeam.com
info@ITSecTeam.com Check for update

Databases:
- MySQL with error
- MySQL no error
- MySQL Blind
- MySQL time based
- MsAccess
- MsAccess Blind
Remote Desktop

TeamSpeak 3 (gaming server)
Common Patterns of Action

- **First Action**: 31%
- **Second Action**: 13%
- **Third Action**: 8%
- **Last Action**: 19%

- **Remote Desktop**: 30%
- **Filesystem**: 24%
- **Webcam, Audio**: 6%
- **Passwords**: 7%

**777 sessions**
Common Patterns of Action

- **Webcam, Audio**: 31%
- **Passwords**: 13%
- **Filesystem**: 8%
- **Remote Desktop**: 11%

**First Action**
- Webcam, Audio: 31%
- Passwords: 13%
- Filesystem: 8%
- Remote Desktop: 11%

**Second Action**
- Webcam, Audio: 11%
- Passwords: 7%
- Filesystem: 7%
- Remote Desktop: 7%

**Third Action**
- Webcam, Audio: 7%
- Passwords: 7%
- Filesystem: 7%
- Remote Desktop: 6%

**Last Action**
- Webcam, Audio: 24%
- Passwords: 19%
- Filesystem: 12%
- Remote Desktop: 19%

In total, 777 sessions were observed.

Webcam, microphone spying always occur early, often first. **System vetting vs. voyeurism?**
Common Patterns of Action

- Webcam, Audio: 31%
- Passwords: 11%
- Filesystem: 13%
- Remote Desktop: 8%

777 sessions

First Action: 30%
Second Action: 24%
Third Action: 19%
Last Action: 12%
Common Patterns of Action

- **Webcam, Audio**: 31%
- **Passwords**: 11%
- **Filesystem**: 19%
- **Remote Desktop**: 12%

First Action: 30%
Second Action: 24%
Third Action: 7%
Last Action: 7%

Filesystem exploration never occurs first; rather, it normally follows (vetting) actions like remote desktop and webcam access.
Common Patterns of Action

777 sessions

First Action:
- Webcam, Audio: 31%
- Passwords: 11%
- Filesystem: 7%
- Remote Desktop: 30%

Second Action:
- Webcam, Audio: 13%
- Passwords: 7%
- Filesystem: 7%
- Remote Desktop: 24%

Third Action:
- Webcam, Audio: 8%
- Passwords: 6%
- Filesystem: 7%
- Remote Desktop: 19%

Last Action:
- Webcam, Audio: 19%
- Passwords: 12%
- Filesystem: 12%
- Remote Desktop: 21%
Password theft occurs most commonly as the last action performed. Goal of operator vs. honeypot exposed?
Common Patterns of Action

- **Webcam, Audio**: 31%
- **Passwords**: 11%
- **Filesystem**: 13%
- **Remote Desktop**: 8%

*First Action*:
- Webcam, Audio: 30%
- Passwords: 24%
- Filesystem: 21%

*Second Action*:
- Webcam, Audio: 7%
- Passwords: 7%
- Filesystem: 7%

*Third Action*:
- Webcam, Audio: 6%
- Passwords: 7%
- Filesystem: 6%

*Last Action*:
- Webcam, Audio: 19%
- Passwords: 12%
- Filesystem: 21%

777 sessions
Overall Trends in Dataset

What **resource(s)** are RAT operators after?

100% .................................................................
75% .................................................................
50% .................................................................
25% .................................................................
0% .................................................................
Overall Trends in Dataset

What **resource(s)** are RAT operators after?

- **61%** With webcam & mic
- **45%** Without (chat, pics, docs)

User Access
Overall Trends in Dataset

What resource(s) are RAT operators after?

- User Access: 61% (45%)
- Credentials: 58%
Overall Trends in Dataset

What **resource(s)** are RAT operators after?
What **resource(s)** are RAT operators after?

- RATs are for user access
What **resource(s)** are RAT operators after?

- RATs are for user access
- RATs are easy, available
Overall Trends in Dataset

What **resource(s)** are RAT operators after?

- RATs are for user access
- RATs are easy, available
- RATs as “gateway”
Further Research Questions
Further Research Questions

Could realistic honeypots serve as a **tar-pit defense** against RAT campaigns?
“[Consume] the attacker[’s] time and effort to no result.”

- The Deception Toolkit
Tarpit Defense

“[Consume] the attacker[’s] time and effort to no result.”

- The Deception Toolkit

- Average interaction: **4 minutes**
- Average remote desktop interaction: **7 minutes**
- **52.9** hours of interaction / **10,800** machine-hours
Tarpit Defense

“[Consume] the attacker[’s] time and effort to no result.”
- The Deception Toolkit

- Average interaction: **4 minutes**
- Average remote desktop interaction: **7 minutes**
- **52.9** hours of interaction / **10,800** machine-hours
- Honeypot realism cost-benefit
Conclusion

• Obtained and decoded 777 interactive sessions with DarkComet operators by executing malware in honeypots
Concluision

- Obtained and decoded 777 interactive sessions with DarkComet operators by executing malware in honeypots

- Attackers seek access to the **victim user**, **credentials**, and **vantage points**

---

I have…a personal laptop. I put a piece of tape over the camera.

- James Comey  
  (former) FBI Director
Conclusion

• Obtained and decoded 777 interactive sessions with DarkComet operators by executing malware in honeypots.

• Attackers seek access to the victim user, credentials, and vantage points.

• RATs enable, encourage amateur “hackers” to cause serious harm to individuals online.
  • We show operator Op-Sec is terrible.
  • Inexpensive honeypots gather attribution information.
  • Law enforcement could use this same technique.

I have…a personal laptop. I put a piece of tape over the camera.

- James Comey (former) FBI Director

“Law enforcement confirms that RATs…are a growing problem.”

- Digital Citizens Alliance
Questions?

Brown Farinholt

UC San Diego

bfarinho@cs.ucsd.edu
Backup Slides
Operator OpSec is Terrible

• 90% of operator IP addresses are **residential** and static

• Attackers often make **no effort to check** if the machine is a honeypot, engage in illegal activity immediately

• Some operators revealed **PII** (which we discarded, IRB) in an attempt to coax us (the victims) into communicating with them

• Some operators visited, even logged into their **personal accounts** in our machines
Related Work

- Honeypots:
  - C. Stoll - *The cuckoo’s egg*

- Low-volume RAT attacks in the wild:
  - Marczak et al. - *When governments hack opponents: A look at actors and technology.*

- RAT criminal community:
  - Digital Citizens Alliance - “Selling slaving”
What is a diurnal pattern?
Victim vs Operator Country

Operator Country

VT Uploader Country

GB  •  •  •  1  •  •  •  •  2  5
FR  •  •  •  •  •  •  •  •  •  11  •
NL  •  •  •  1  •  •  •  •  2  2  •
TH  •  •  •  1  •  •  •  •  13  •  6  •
BR  •  •  •  •  •  •  •  •  •  2  •  5  •
US  •  •  •  •  •  •  •  •  •  16  1  •  •  •  4  •
UA  •  •  •  9  •  •  •  •  8  •  3  •  •  •  •  7  •
TR  •  •  •  50  •  •  •  •  3  •  1  •  •  •  •  13  •
RU  •  •  •  32  •  •  •  •  1  •  3  •  •  •  •  •  •  20  •

RU  TR  UA  US  BR  TH  NL  FR  GB
Further Research Questions

Could realistic honeypots serve as a **tar-pit defense** against RAT campaigns?
Further Research Questions

Could realistic honeypots serve as a tar-pit defense against RAT campaigns?

Do RAT operators unwittingly give up threat intelligence in compromised systems?
Threat Intelligence: Technical indicators about threats that can inform defenses and/or identify actors and infrastructure.
Threat Intelligence: Technical indicators about threats that can inform defenses and/or identify actors and infrastructure

Attackers…

- Visited **123** URLs
- Dropped **34** executables
- Used **13** different honey-credentials offline
- Offered **PII**, used **ACTUAL CREDENTIALS**
Attackers…

- Visited **123** URLs
- Dropped **34** executables
- Used **13** different honey-credentials offline
- Offered **PII**, used **ACTUAL CREDENTIALS**

**Threat Intelligence**: Technical indicators about threats that can inform defenses and/or identify actors and infrastructure

**Attack Attribution**