TURNING DECEPTION OUTSIDE-IN

TRICKING ATTACKERS WITH OSINT
About Us

Security Researchers at Illusive Networks

- Hadar Yudovich (@hadar0x)
- Tom Kahana (@tomkahan1)
- Tom Sela (@4x6hw)
Agenda

● OSINT
  ○ How attackers use OSINT
  ○ What defenders do about OSINT

● Deceptions

● OSINT Deceptions - Our Research
  ○ Setting up an environment
  ○ Deceptions Planting
  ○ Findings

● Summary / Takeaways
Open-source intelligence (OSINT) is data collected from publicly available sources to be used in an intelligence context...”

Wikipedia
Attacks ❤ Open Source Intelligence

- **OSINT** is mainly used for Reconnaissance before a network infiltration

- **Collected Info**
  - IP Addresses
  - Emails
  - Configs
  - Scripts
  - Usernames
  - Passwords
  - Credential Dumps
  - API Keys
  - Personal Information

- **Resources**
  - Search Engines
  - Paste Sites
  - Social Networks
  - WHOIS Sites
  - Code Repositories
  - Virustotal

- **Existing tools**
  - **Open Source**: theHarvester, recon-ng, datasploit, PasteHunter
  - **Commercial**: Maltego, Shodan, VirusTotal Retrohunt
OSINT In The Wild

I made the same mistake. I had the keys in a CRON job file that must have got through my .gitignore file. I now have $50,000 in AWS charges. Contacted Amazon and shut everything down and deleted my keys (which were deactivated but not in every region).

I really hope this gets reversed because I've only ever had a Micro server running and these charges all accumulated in 4 days.

By Andrew

Exposed within this repository are not only passwords and manifests for Viacom's servers, data needed to maintain and expand the IT infrastructure of an $18 billion multinational corporation, but perhaps more significantly, Viacom's access key and secret key for the corporation's AWS account. By exposing these credentials, control of Viacom's servers, storage, or databases under the AWS account could have been compromised. Analysis reveals that a number of cloud instances used within Viacom's IT toolchain, including Docker, New Relic, Splunk, and Jenkins, could've thus been compromised in this manner.
Defenders ❤️ OSINT

● What defenders usually do with data found in OSINT resources?
  ○ PANIC MODE
  ○ Try to “remove” it from the internet - not easy
  ○ Try to disable / make the exposed data obsolete - not always easy

● What defenders could also do?
  ○ TRICK ATTACKERS WITH OSINT DECEPTIONS
Deceptions

- Deception in modern warfare
- Digital Deceptions (a.k.a bread-crums, lures, honeytokens, etc.)

Detecting attackers with digital deceptions
  - Plant Windows LSASS Credentials
  - Applicative Saved Credentials (SSH/FTP/DB Clients)
  - Attempt to use the credentials == alert
Deceptions

- Deception in modern warfare
- Digital Deceptions (a.k.a. bread-crums, lures, honeytokens, etc.)

- Detecting attackers with digital deceptions
  - Plant Windows LSASS Credentials
  - Applicative Saved Credentials (SSH/FTP/DB Clients)
  - Attempt to use the credentials == alert

- Intranet VS Internet facing deceptions
**Open Source Intelligence + Deceptions = ❤️**

- Collected Info
  - IP Addresses
  - Emails
  - Configs
  - Scripts
  - Usernames
  - Passwords
  - Credentials Dump
  - API Keys
  - Personal Information

- Resources
  - Search Engines
  - Paste Sites
  - Social Networks
  - WHOIS Sites
  - Code Repositories
  - Virustotal
Thesis

- Attackers use OSINT
  - Network Compromise
  - Post Breach Lateral Movement
Steps

- Started a front organization
- Built an environment
- Planted different deceptive information in different OSINT resources
- Monitored Activity
Step #1 - Front Organization
Step #2 - Network Environment

- Cloud based, domain joined computers & servers
- Jump Server - **Entry Point (Internet Facing)**
- Controlled & Monitored
Step #3 - Deception Planting

- **What do we plant?**
  - Internal Resources (IPs, Hostnames, URLs)
  - Credentials (Usernames + Passwords, API Keys, Applications’ Config Files)
  - Credentials Dumps (NTDS.dit Dump, Mimikatz Dump)

- **Where do we plant? (examples)**
  - Paste Sites - Pastebin
  - Public Email Mailboxes - Mailinator
  - Code Repositories - GitHub
  - File Uploads - Virustotal
PasteBin

rdp - 35.195.187.217
mfreitas@aviatomining.com:nujnsvuteeh33!
Your password has been changed

Dear Erlich Stone,

Your Password Has Been Changed!

This email confirms that your password has been changed.

To log on to the site, use the following credentials:

Username: estone
Password: H^j@K28

If you have any questions or encounter any problems logging in, please contact a site administrator.
removed my password and replaced with prompt for pass

```powershell
#$password = "hT@russel@tH123!"
+$password = Read-Host -Prompt "Enter Your Password"
```
Virustotal

We found 1 hashes! [Timer: 716 m/s] Please find them below...

c39f2beb3d2ec06a62cb887fb391dee0 NTLM: Password2
Many More

- RDP Shops
- GitHub Gists
- Cloud Storage - Google, Amazon S3
- IRC Channels
- Hacking Forums, Reddit
All Together Now - BEFORE

Your search - aviatomicing.com - did not match any documents.

Suggestions:
- Make sure that all words are spelled correctly.
- Try different keywords.
- Try more general keywords.

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

rbrown@aviatomicing.com

Good news — no pwnage found!
No breached accounts and no pastes (subscribe to search sensitive breaches)
All Together Now - AFTER
Step #4 - Monitoring

- We ran the experiment for ~2 months
- Used unique identifiers for each resource to easily detect the source
- Monitoring focused on usage of deceptions and attempts to move laterally
  - (Although we did encounter other things)
Findings Overview

- **7,952** Successful logins with our deceptive usernames
- **723** Distinct processes were executed
- **19,762** Failed login attempts of non-existing users (scanners)
Findings - Paste Sites Use Case

- Most monitored site - PasteBin.com
- Time diff between deception planting and attacker attempt to use them
  - Fastest of all OSINT resources
  - 4 Hours
- Exposure Monitoring
  - Maximum Views - 7000~ in 1 month
  - 40~ views after several minutes (non human?)
- Scraped automatically by many different tools
  - DumpMon, Have I Been Pwned, PasteHunter, etc.
  - Attempts to use the deceptive users decreased daily
Findings - GitHub Use Case

- Time diff between deception planting and attacker attempt to use them
  - Days

- Exposure Monitoring
  - 10s of views

- Automatic Tools
  - Tools only scan specific repositories and do not scrape in scale
  - reposcanner, gitrob
Findings - Entry Point Activities

- Lateral Movement / Enumeration
  - net commands (users, groups, etc.)

- Privilege Escalation
  - Keylogger + Windows Notification (wlrmdr.exe)
  - CVE-2016-0099

- Generally Malicious Tools
  - Sentry MBA
  - DDoS Bot
  - 3 Bitcoin Miners
  - Traffic Spirit

- Weird Stuff
Summary

● We Covered
  ○ OSINT & Deceptions
  ○ Our Research - Thesis, Steps
  ○ Research Results *

● Conclusions
  ○ Human operators and not automatic scrapers\bots
  ○ It can take only 4 hours to knock on your door
  ○ Deception authenticity
  ○ “Honey Organization” is not the same as “Real Organization”
  ○ Will it increase attack surface?

* Full report will be published on the Illusive Labs website - https://blog.illusivenetworks.com/tech
Takeaways

- **Run OSINT tools against your organization** - you may be surprised of what you find

- **Turn the problem to an advantage** - if you have leaked information about your organization in OSINT resources, use it for detection

- **Plant new OSINT deceptions** to increase your detection capabilities
Questions?