TURNING DECEPTION OUTSIDE-IN

TRICKING ATTACKERS WITH OSINT

About Us

Security Researchers at Illusive Networks

- Hadar Yudovich (@hadar0x)
- Tom Kahana (@tomkahana1)
- Tom Sela (@4x6hw)

illusive™

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

OSINT

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

Wikipedia

Attackers ❤ 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

Wed, July 15, 2015 9:02am

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

https://securosis.com/blog/my-500-cloud-security-screwup

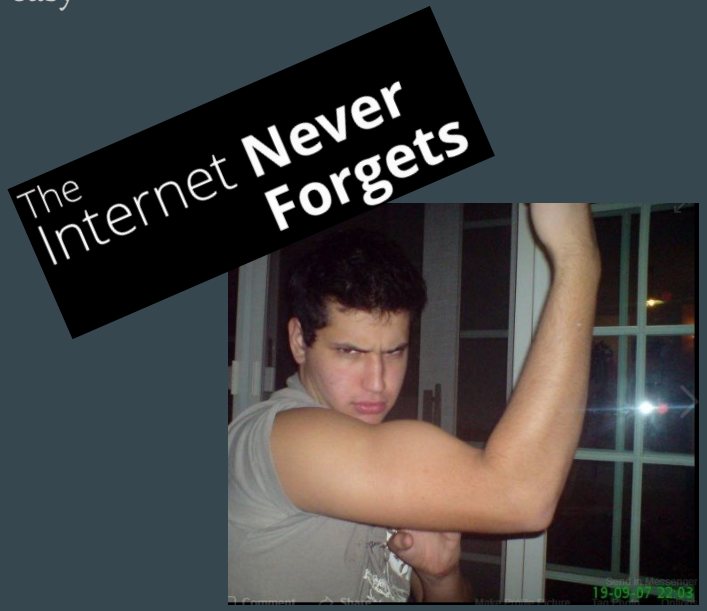
Exposed within this repository are not only passwords and manifests for Viacom's servers, data needed to maintain and expand the IT infrastructure of an $18 billion multinational corporation, but perhaps more significantly, Viacom's access key and secret key for the corporation's AWS account. By exposing 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.

https://www.upguard.com/breaches/cloud-leak-viacom

Defenders 💔 OSINT

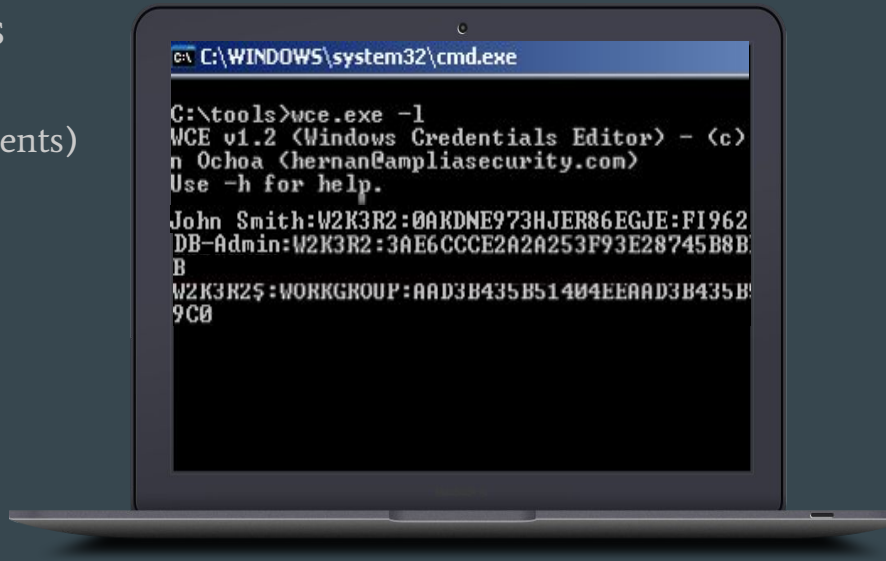
- What defenders usually do with data found in OSINT resources?
  - PANIC MODE
  - Try to “remove” it from the internet - not easy
  - Try to disable / make the exposed data obsolete - not always easy

- What defenders could also do?
  - **TRICK ATTACKERS WITH OSINT DECEPTIONS**



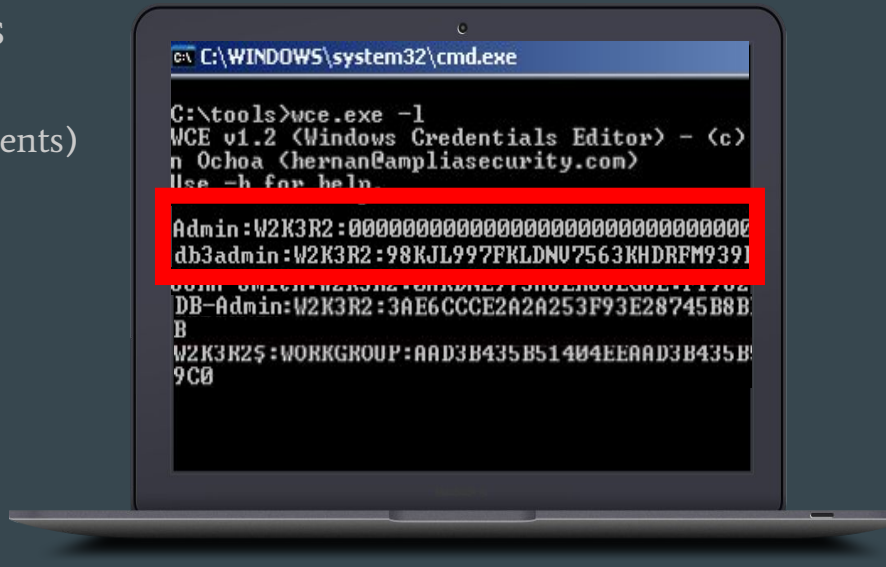
Deceptions

- Deception in modern warfare
- Digital Deceptions (a.k.a bread-crumbs, 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-crumbs, 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

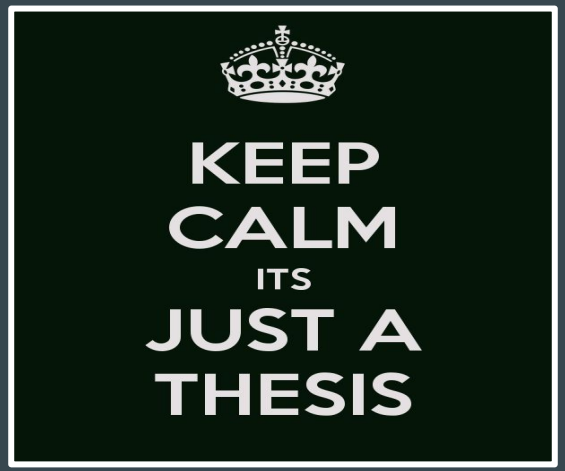


Open Source Intelligence + Deceptions = ❤

- 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

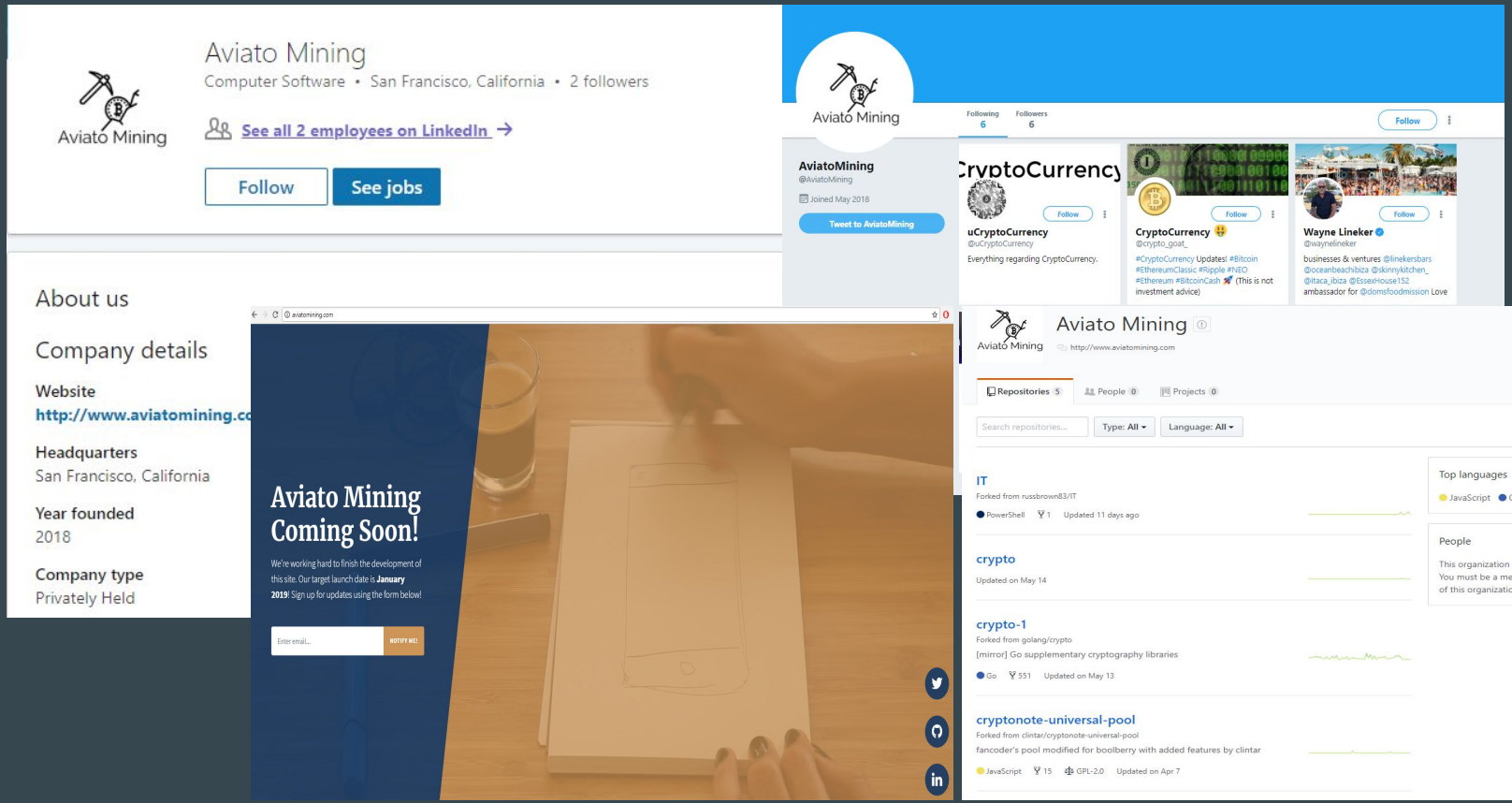
- Attackers use OSINT
  - Network Compromise
  - Post Breach Lateral Movement



Steps

- Started a front organization
- Built an environment
- Planted **different** deceptive information in **different** OSINT resources
- Monitored Activity

Step #1 - Front Organization



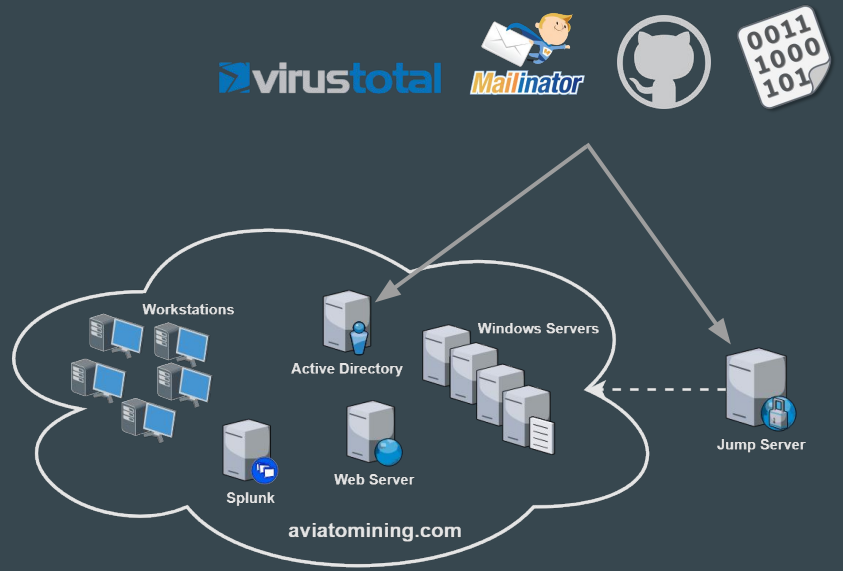
Step #2 - Network Environment

- Cloud based, domain joined computers & servers
- Fake Users & Computers Objects (https://github.com/RobBridgeman/ADImporter)
- 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

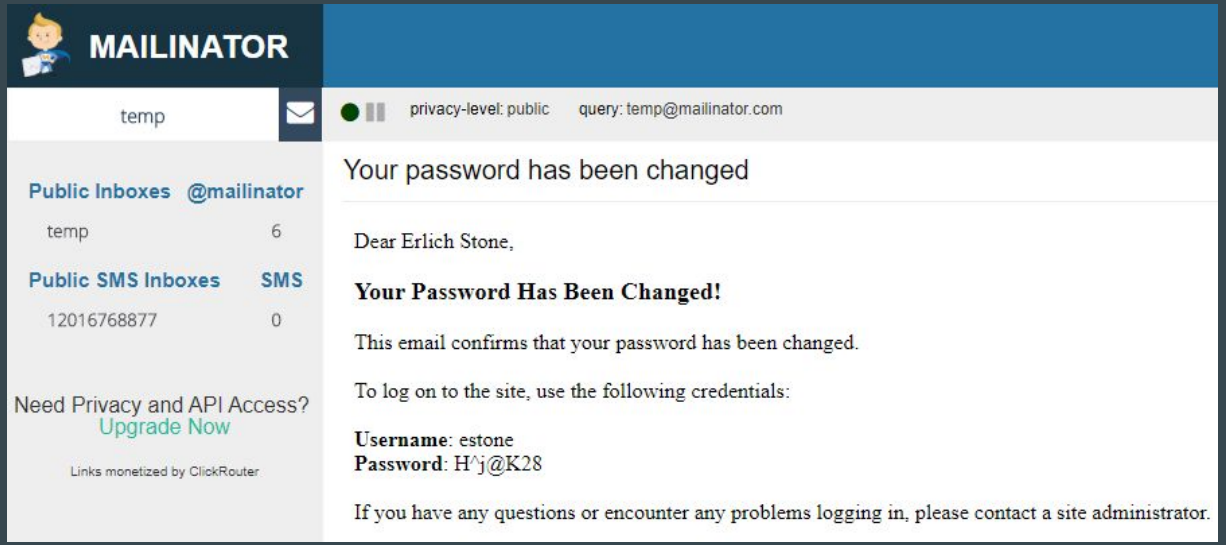


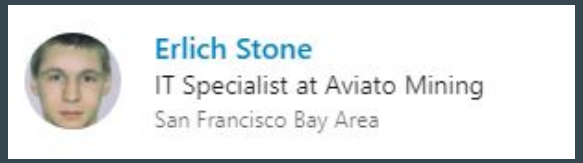
PasteBin

rdp - 35.195.187.217

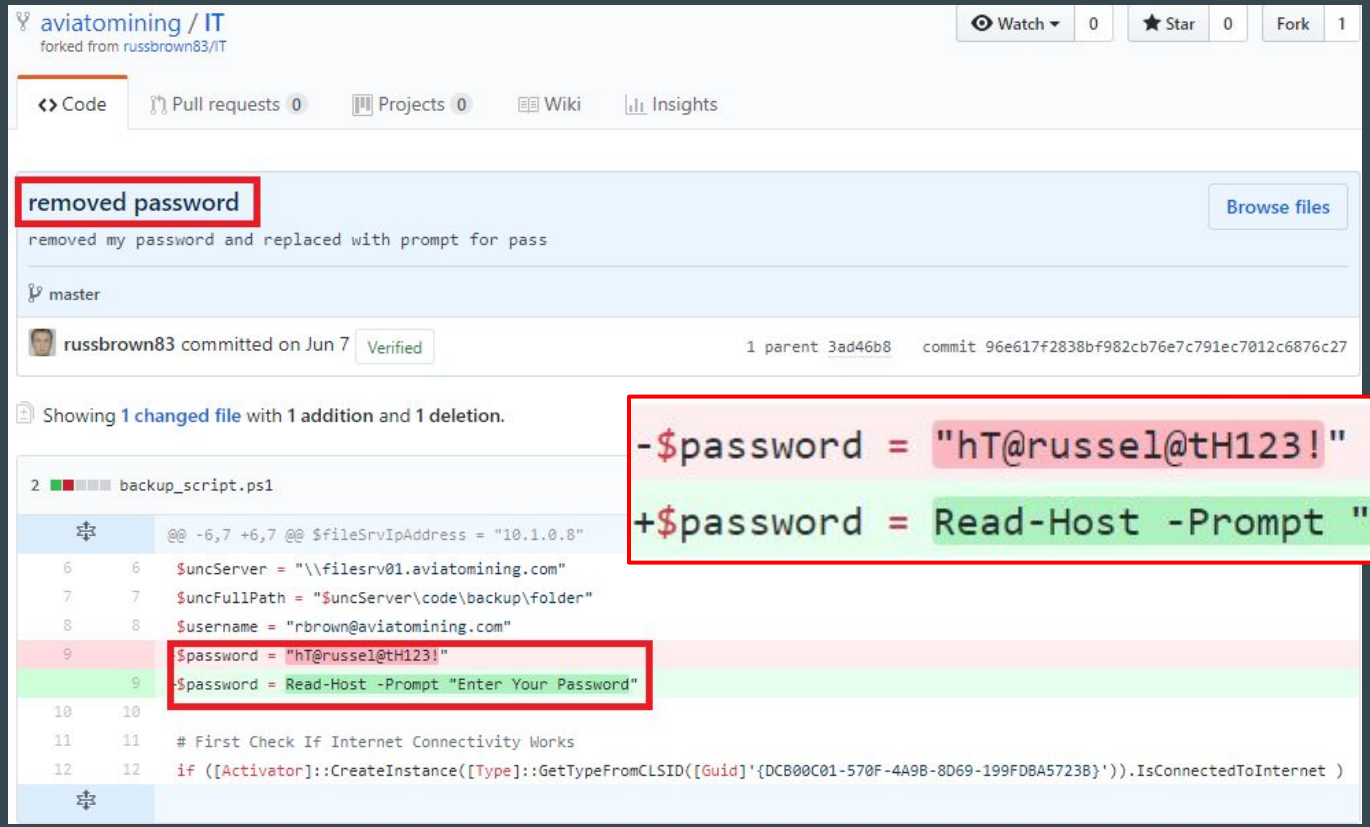
mfreitas@aviatomining.com:nujnsvuteeh33!

Mailinator


MAILINATOR
temp
privacy-level: public
query: temp@mailinator.com
Public Inboxes @mailinator
temp 6
Public SMS Inboxes SMS
12016768877 0
Need Privacy and API Access?
Upgrade Now
Links monetized by ClickRouter
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.

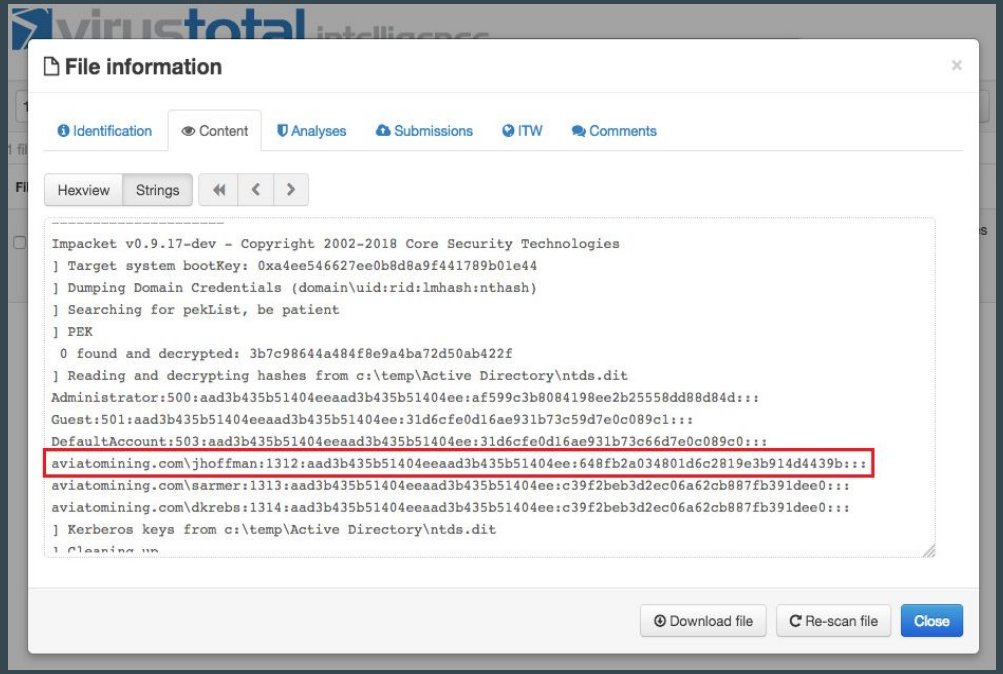

Erlich Stone
IT Specialist at Aviato Mining
San Francisco Bay Area

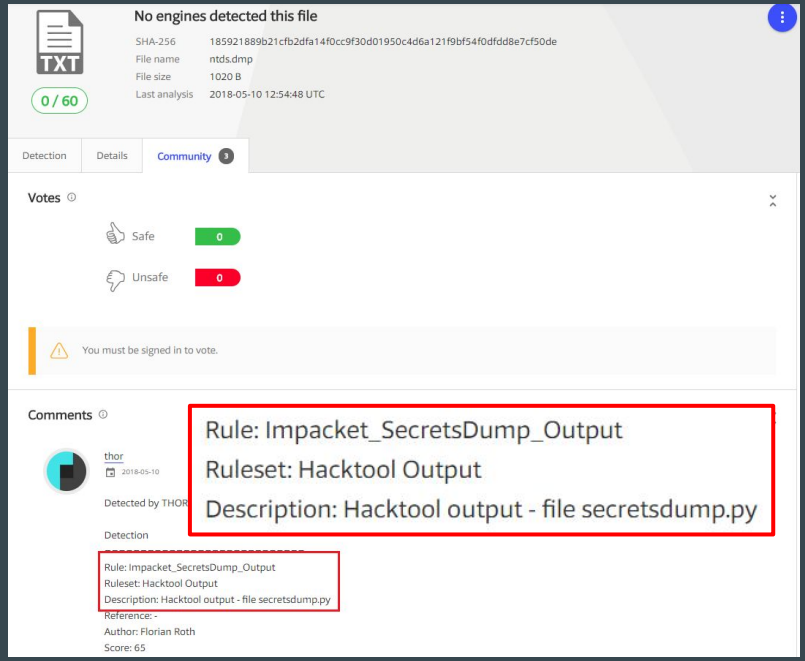
GitHub

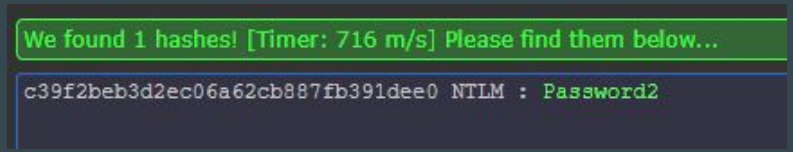



```
-$password = "hT@russel@tH123!"
+$password = Read-Host -Prompt "Enter Your Password"
```

Virustotal


File information
Identification
Content
Analyses
Submissions
ITW
Comments
Hexview
Strings
Impacket v0.9.17-dev - Copyright 2002-2018 Core Security Technologies
] Target system bootKey: 0xa4ee546627ee0b8d8a9f441789b01e44
] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
] Searching for pekList, be patient
] PEK
0 found and decrypted: 3b7c98644a484f8e9a4ba72d50ab422f
] Reading and decrypting hashes from c:\temp\Active Directory\ntds.dit
Administrator:500:aad3b435b51404eeaad3b435b51404ee:af599c3b8084198ee2b25558dd88d84d:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c1:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c66d7e0c089c0:::
aviatomining.com\jhoffman:1312:aad3b435b51404eeaad3b435b51404ee:648fb2a034801d6c2819e3b914d4439b:::
aviatomining.com\sarmer:1313:aad3b435b51404eeaad3b435b51404ee:c39f2beb3d2ec06a62cb887fb391dee0:::
aviatomining.com\dkrebs:1314:aad3b435b51404eeaad3b435b51404ee:c39f2beb3d2ec06a62cb887fb391dee0:::
] Kerberos keys from c:\temp\Active Directory\ntds.dit
Download file
Re-scan file
Close

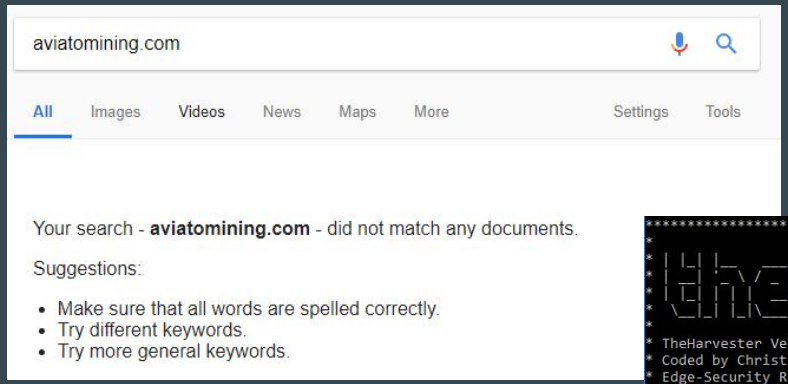

No engines detected this file
TXT
0 / 60
SHA-256 185921889b21cfb2dfa14f0cc9f30d01950c4d6a121f9bf54f0dfdd8e7cf50de
File name ntds.dmp
File size 1020 B
Last analysis 2018-05-10 12:54:48 UTC
Detection
Details
Community 3
Votes
Safe 0
Unsafe 0
You must be signed in to vote.
Comments
thor
2018-05-10
Detected by THOR
Detection
Rule: Impacket_SecretsDump_Output
Ruleset: Hacktool Output
Description: Hacktool output - file secretsdump.py
Reference: -
Author: Florian Roth
Score: 65
Rule: Impacket_SecretsDump_Output
Ruleset: Hacktool Output
Description: Hacktool output - file secretsdump.py

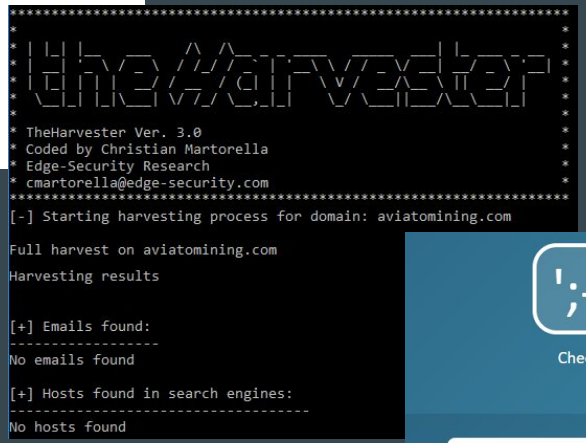

We found 1 hashes! [Timer: 716 m/s] Please find them below...
c39f2beb3d2ec06a62cb887fb391dee0 NTLM : Password2

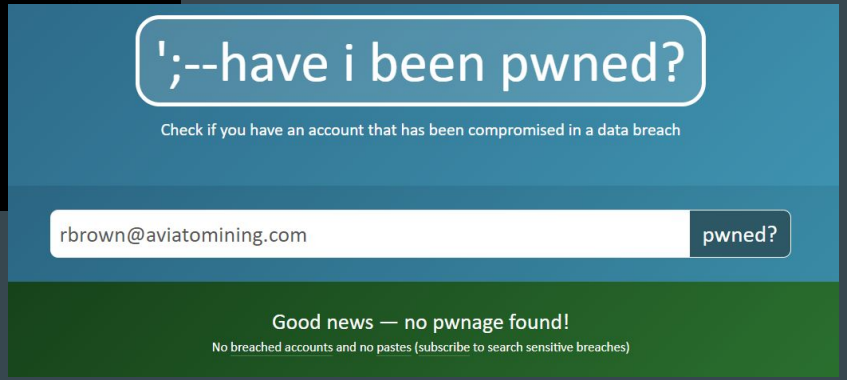
Many More

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

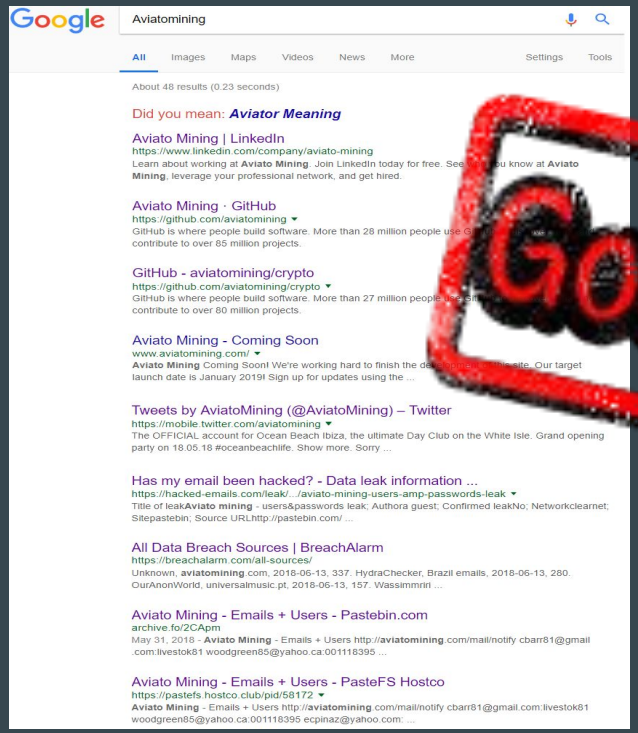
All Together Now - **BEFORE**

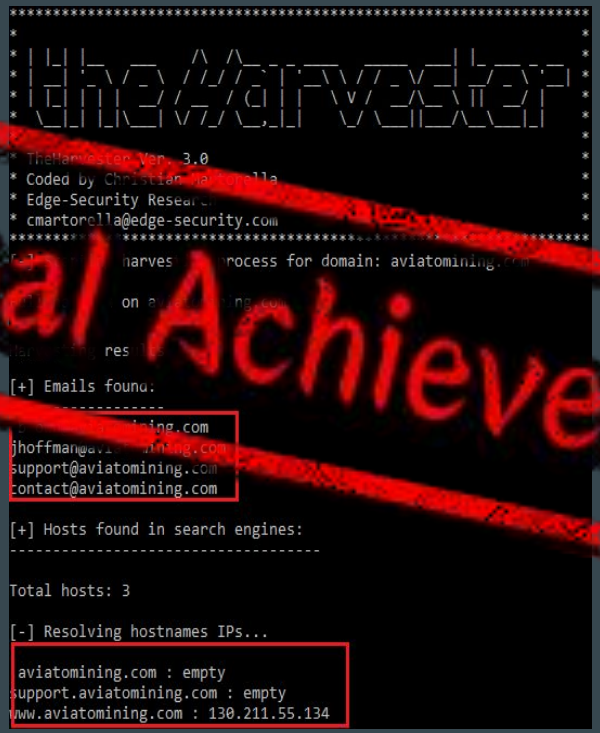


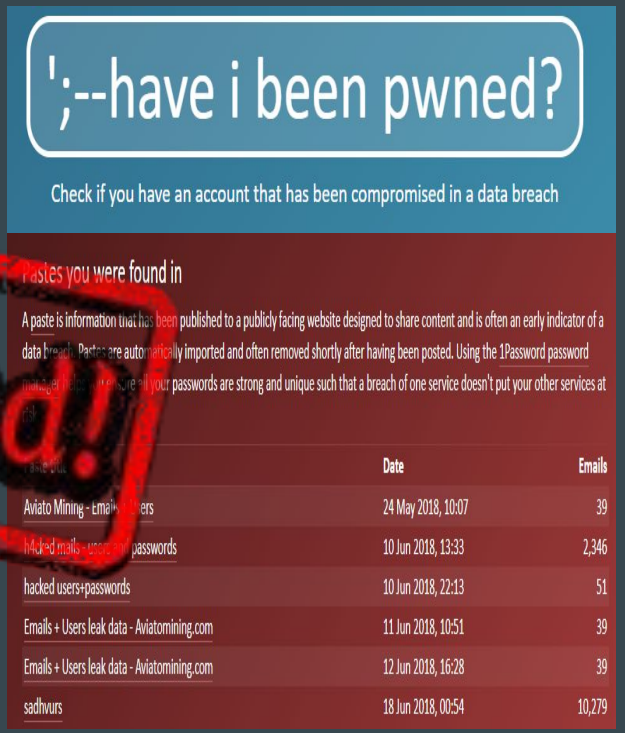




All Together Now - **AFTER**







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?)

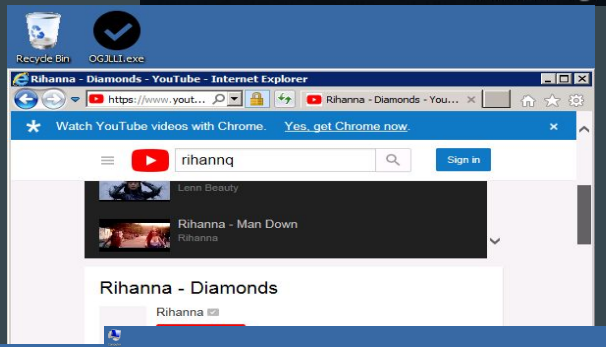
- Scraped automatically by many different tools
  - DumpMon, Have I Been Pwned, PasteHunter, etc.
  - Attempts to use the deceptive users decreased daily

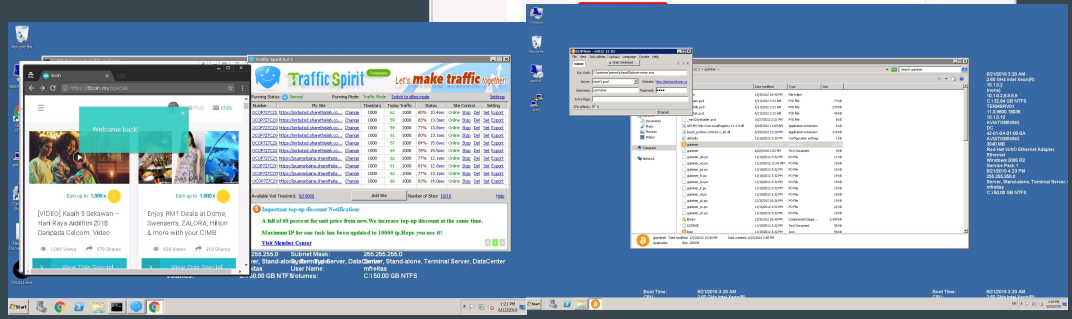
Findings - GitHub Use Case

- 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?