Inside Cybercrime Groups Harvesting Active Directory for Fun and Profit - Vitali Kremez

Archived: 2026-04-05 22:49:25 UTC

Automated Malware + Interactive Human Exploitation Operator

Emotet (Loader for Installs) -> **TrickBot** -> **Ryuk Ransomware** (via PowerShell Empire/Cobalt Strike)

...Network & Active Directory Parsing!....

Reference: "Charting the Next Cybercrime Frontier, or Evolution of Criminal Intent
https://www.youtube.com/watch?v=pfL0aTYzRM
Credit: Ryuk image (https://hogarthsp.com/products/ryuk)

Scope of TrickBot Installs: How Big is the Problem?

Newer Cybercrime Frontier: TrickBot Makes Headlines with Ryuk Install via Active Directory

What is **Ryuk**, the malware believed to have hit the Los Angeles **Times**?
Los Angeles Times - Jan 1, 2019
Ryuk, a malware program believed to have been used in an attack this ... hobbled newspapers nationwide, including the Los Angeles **Times**, ...

Ryuk ransomware attack delays the distribution of major US newspapers
2-spyware.com (blog) - Jan 2, 2019

Major US newspapers crippled by **Ryuk** ransomware attack
CSO Online - Jan 2, 2019

TrickBot in the Cloud: CloudJumper MSP Intrusion: $5 Billion Extortion Amount in Total (!)

Reference:
https://twitter.com/barton_paul/status/1127068679132987394

TrickBot Makes Headlines with Ryuk Install via Active Directory: CloudJumper MSP

Breached MSP Victim –>
Gateway to Other Organization Cloud Infrastructure

Active Directory Kill Chain Attack & Defense

Credit:
Rahmat Nurfauzi (https://github.com/infosecn1nja/AD-Attack-Defense/blob/master/README.md)

Active Directory Enumeration & Exploitations

Active Directory Enumeration Methodologies

domainDll (32/64)

- "domainDll32," compiled via 'GCC: (Rev1, Built by MSYS2 project) 7.2.0,' allows TrickBot operators to collect domain controller information once they are already on the compromised machine.
- This module is internally called "DomainGrabber" and accepts command "getdata" in order to start harvest domain information.
- domainDll appears to be aimed at exploiting networks with unsecured domain controllers.

Reference: https://www.vkremez.com/2017/12/lets-learn-introducing-new-trickbot.html

Active Directory Enumeration Methodologies

domainDll (32/64) (decoded)
(1e2791877da0249998dea79515a89ca)

Active Directory Enumeration Methodologies

domainDll (32/64)

Active Directory Enumeration Methodologies

networkDll (32/64)

- "**networkDll**" module is a single harvester of all possible network victim information from running commands such as "ipconfig /all" and "nltest /domain_trusts /all_trusts" to WMI Query Language (WQL) queries such as "SELECT * FROM Win32_OperatingSystem" to lightweight directory access protocol (LDAP) queries.
- Notably, the group leverages "nltest" commands to establish trust relationship between between a compromised workstation and its possible domain before querying LDAP.

Reference:
https://www.vkremez.com/2018/04/lets-learn-trickbot-implements-network.html

Active Directory Enumeration Methodologies

networkDll (32/64) (decoded)
(aeb08b0651bc8a13dcf5e5f6c0d48218)

LDAP network and domain queries

Active Directory Enumeration Methodologies

c nfidence

networkDll (32|64)

Active Directory Enumeration Methodologies

c nfidence

psfinDll (32|64)

- "**psfin32**" is a point-of-sale finder reconnaissance module hunts for point of sale related services, software, and machines in Lightweight Directory Access Protocol (LDAP)
- The module itself does not steal any point-of-sale data but rather used to profile corporate machines of interest with possible point-of-sale devices.
- This module arrived just in time for the holiday shopping season highlighting the group interest in exploring possible point-of-sale breaches.

Reference:
https://www.vkremez.com/2018/11/lets-learn-introducing-latest-trickbot.html

Active Directory Enumeration Methodologies

c nfidence

psfinDll (32|64): Typical Point-of-Sale Network Layout

Credit:
https://www.smart-acc.com/?page=size-options/multiple-outlets/retail

Active Directory Enumeration Methodologies

c nfidence

psfinDll (32|64)
(4fce2da754c9a1ac06ad11a46d215d23)

Active Directory Enumeration Methodologies

c nfidence

psfinDll (32|64)

LDAP provider is used to access Active Directory domain services. The LDAP binding string takes the following form of "GC://" binding to the root of the namespace. "GC:" uses the LDAP provider to bind to the Global Catalog service to execute queries.
The module queries for DOMAIN Global Catalog the following accesses:

```
COMPUTERS
USERS
GROUPS
SITES
DCs
```

The point-of-note key terms of interest are as follows:

```
*DCS*
*DES*
*CASE*
*GAME*
*VICTIM*
*NETBIOS*
*NEW*
*YELLOW*
*MICROSOFT
*YEARN*
```

c nfidence

Life Cycle of High-Profile Event: Typical Exploitation Chain & Tactics, Techniques & Procedures

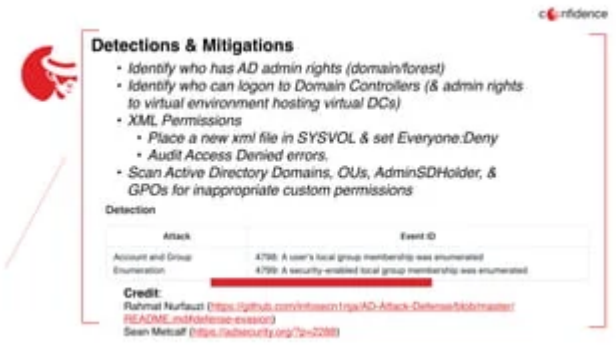
Credit:
Brad Duncan (https://www.malware-traffic-analysis.net/2018/10/08/index.html)

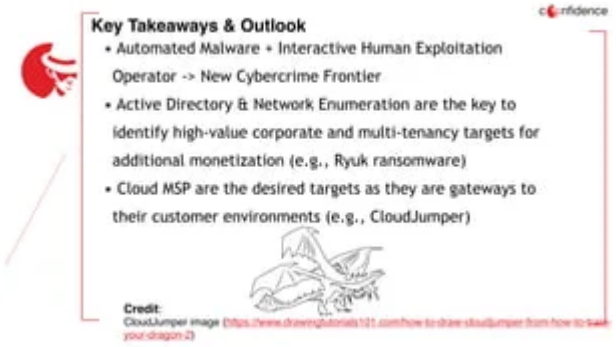
c nfidence

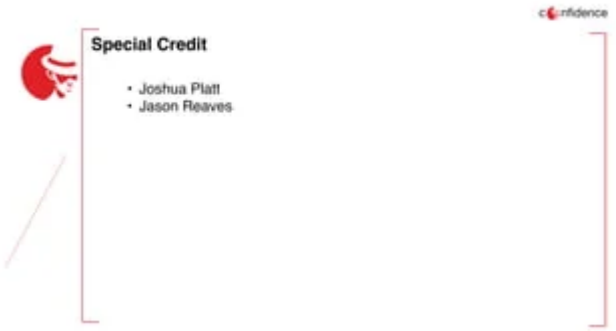
Life Cycle of High-Profile Event: Victim Domain Parser

c nfidence

Life Cycle of High-Profile Event: "No system is safe"







More Related Content

PDF

BSides IR in Heterogeneous Environment

PDF

[HITCON 2020 CTI Village] Threat Hunting and Campaign Tracking Workshop.pptx

PDF

[CB19] Cyber Threat Landscape in Japan – Revealing Threat in the Shadow by C...

PDF

MITRE ATTACKCon Power Hour - December

PDF

MITRE ATT&CKcon 2018: Playing Devil’s Advocate to Security Initiatives with A...

PDF

ATT&CKING Containers in The Cloud

PDF

MITRE ATT&CKcon 2018: Sofacy 2018 and the Adversary Playbook, Robert Falcone,...

PDF

David Bianco - Enterprise Security Monitoring

What's hot

PPTX

BSidesLV 2016 - Powershell - Hunting on the Endpoint - Gerritz

PDF

"Is your browser secure? Breaking cryptography in PKI based systems, opening ...

PPTX

Corporate Espionage without the Hassle of Committing Felonies

PDF

Helping Small Companies Leverage CTI with an Open Source Threat Mapping

PDF

"Giving the bad guys no sleep"

PDF

Offensive malware usage and defense

PDF

When Insiders ATT&CK!

PPTX

Malware Static Analysis

PPTX

"There's a pot of Bitcoins behind the ransomware rainbow"

PDF

MITRE ATT&CKcon 2.0: Ready to ATT&CK? Bring Your Own Data (BYOD) and Validate...

PDF

Shamoon

PDF

Catching the Golden Snitch- Leveraging Threat Intelligence Platforms to Defen...

PDF

MITRE ATT&CKcon 2018: Detection Philosophy, Evolution & ATT&CK, Fred Stankows...

PDF

The 4horsemen of ics secapocalypse

PPTX

Conclusions from Tracking Server Attacks at Scale

PDF

Insider Threat Visualization - HITB 2007, Kuala Lumpur

PDF

Wannacry | Technical Insight and Lessons Learned

PPTX

Using GreyNoise to Quantify Response Time of Cloud Provider Abuse Teams

PDF

Sharpening your Threat-Hunting Program with ATTACK Framework

PDF

PHDays 2018 Threat Hunting Hands-On Lab

Similar to Inside Cybercrime Groups Harvesting Active Directory for Fun and Profit - Vitali Kremez

PDF

theVIVI-AD-Security-Workshop_AfricaHackon2019.pdf

PPTX

Catch Me If You Can - Finding APTs in your network

PPTX

Implementing Active Directory and Information Security Audit also VAPT in Fin...

PPTX

Bridging the Gap

PPTX

Go Hack Yourself - 10 Pen Test Tactics for Blue Teamers

PDF

ADRecon - Detection CHCON 2018

PPTX

BSides SG Practical Red Teaming Workshop

PPTX

BSIDES-PR Keynote Hunting for Bad Guys

PDF

Windows Threat Hunting

PPTX

Hybrid Active Directory Cyber Resiliency

PPTX

Adversarial Post-Ex: Lessons From The Pros

PPTX

Adversarial Post Ex - Lessons from the Pros

PPTX

Scrapping for Pennies: How to implement security without a budget

PDF

I Have the Power(View)

PDF

DEF CON 24 - Sean Metcalf - beyond the mcse red teaming active directory

PPTX

Windows advanced

PPTX

Kyle Taylor – increasing your security posture using mc afee epo

PPTX

I hunt sys admins 2.0

PPTX

Defending Your "Gold"

PDF

Hacking our chairmans inbox - Charl van der Walt - SensePost

Recently uploaded

PDF

Secure Java Applications against Quantum Threats

PDF

Động cơ hơi nước đôi bản vẽ chi tiết và bản vẽ lắp

PDF

How a Gated Community Operates on Ground?

PDF

Empowering BFSI with ThousandEyes Real-Time Digital Performance Intelligence

PDF

2025 Infrastructure Resilience Blueprint

PDF

Energy Aware Combinatorial Optimization.pdf

PPTX

Collaborating with UX to Embed Accessibility in Design Workflows

PPTX

Hyper-Aether: AI-Native Computing with Dynamic VM Fabric Architecture

PDF

Data-Driven-Security-in-Gated-Communities.pptx.pdf

PDF

Information Retrieval systems-(RAG).2026.Sec-(4)-(6)

PDF

Agent Orchestration using GitHub Copilot

PPTX

Automating Form Validation and Verification with Multi-Modal LLMs

PDF

Jos-BwAI26_Umar_Faruq_Zubairu_Build and Deploy a Multi-Agent Guide on Cloud R...

PDF

Comprehensive Guide to Matplotlib for Python Data Visualization

PPTX

Comprehensive Guide to Access Control and Security Vulnerabilities

PDF

The Automated Factory A Strategic Blueprint for Modern Production Workflows

PDF

Defending Against Generative Malware & Deepfakes in Cognitive Security Era

PPTX

Comprehensive Introduction to Blockchain Technology for Maritime Sector Appli...

PDF

Is Your Society Ready for 2026: A quick checklist for modern gated communities

PDF

HCL Notes 2026: New User Experience Deep Dive

Inside Cybercrime Groups Harvesting Active Directory for Fun and Profit - Vitali Kremez

- 1.
- 2.

  Introducing Cybercrime Groups Talk Outline 1 3 TrickBotin the Cloud: CloudJumper MSP Intrusion Active Directory Enumeration Methodologies 2 4 Life Cycle of High- Profile Event: Typical Exploitation & TTPs 5 Detections & Mitigations 5 Key Takeaways & Outlook

- 3.

  Cybercrime Enterprise Dealwith Big Data • Sophisticated criminal enterprises such as TrickBot & QakBot - focused on parsing and identifying high-value targets (HVT) • Need reliable install loaders - intermittently rely on Emotet Loader for installs • Big botnet data collectors necessitate scalable solutions to identify high-value targets (corporate networks with local domains) versus “useless” infections • Simple idea: Squeeze as £ / € / $ value from your bots as possible • Banking Malware • Credential Stealer • Miner • Ransomware! Reference: “Charting the Next Cybercrime Frontier, or Evolution of Criminal Intent https://www.youtube.com/watch?v=ptL0aTYzRfM

- 4.

  Cybercrime Enterprise Dealwith Big Data Reference: “Charting the Next Cybercrime Frontier, or Evolution of Criminal Intent https://www.youtube.com/watch?v=ptL0aTYzRfM

- 5.

  Emotet (Loader forInstalls) -> TrickBot -> Ryuk Ransomware (via PowerShell Empire/Cobalt Strike) Reference: “Charting the Next Cybercrime Frontier, or Evolution of Criminal Intent https://www.youtube.com/watch?v=ptL0aTYzRfM Credit: Ryuk image (https://nogiartshop.com/products/ryuk) …Network & Active Directory Parsing!…. Automated Malware + Interactive Human Exploitation Operator

- 6.

- 7.
- 8.

  TrickBot in theCloud: CloudJumper MSP Intrusion $5 Billion Extortion Amount in Total (!) Reference: https://twitter.com/barton_paul/status/1127088679132987394

- 9.

  TrickBot Makes Headlineswith Ryuk Install via Active Directory: CloudJumper MSP Breached MSP Victim —> Gateway to Other Organization Cloud Infrastructure

- 10.
- 11.
- 12.

  • "domainDll32," compiledvia 'GCC: (Rev1, Built by MSYS2 project) 7.2.0,' allows TrickBot operators to collect domain controller information once they are already on the compromised machine. • This module is internally called "DomainGrabber" and accepts command "getdata" in order to start harvest domain information. • domainDll appears to be aimed at exploiting networks with unsecured domain controllers. domainDll (32|64) Reference: https://www.vkremez.com/2017/12/lets-learn-introducing-new-trickbot.html Active Directory Enumeration Methodologies

- 13.
- 14.
- 15.

  Active Directory EnumerationMethodologies • “networkDll” module is a single harvester of all possible network victim information from running commands such as "ipconfig /all" and "nltest /domain_trusts /all_trusts" to WMI Query Language (WQL) queries such as "SELECT * FROM Win32_OperatingSystem" to lightweight directory access protocol (LDAP) queries. • Notably, the group leverages "nltest" commands to establish trust relationship between between a compromised workstation and its possible domain before querying LDAP. networkDll (32|64) Reference: https://www.vkremez.com/2018/04/lets-learn-trickbot-implements-network.html

- 16.
- 17.
- 18.

  • “psfin32” isa point-of-sale finder reconnaissance module hunts for point of sale related services, software, and machines in Lightweight Directory Access Protocol (LDAP) • The module itself does not steal any point-of-sale data but rather used to profile corporate machines of interest with possible point-of-sale devices. • This module arrived just in time for the holiday shopping season highlighting the group interest in exploring possible point-of-sale breaches. psfinDll (32|64) Reference: https://www.vkremez.com/2018/11/lets-learn-introducing-latest-trickbot.html Active Directory Enumeration Methodologies

- 19.

  psfinDll (32|64): TypicalPoint-of-Sale Network Layout Credit: https://www.smart-acc.com/?page=size-options/multiple-outlets/retail Active Directory Enumeration Methodologies

- 20.
- 21.
- 22.

  Life Cycle ofHigh-Profile Event: Typical Exploitation Chain & Tactics, Techniques & Procedures Credit: Brad Duncan (https://www.malware-traffic-analysis.net/2018/10/08/index.html)

- 23.

  Life Cycle ofHigh-Profile Event: Victim Domain Parser

- 24.
- 25.

  Detections & Mitigations •Identify who has AD admin rights (domain/forest) • Identify who can logon to Domain Controllers (& admin rights to virtual environment hosting virtual DCs) • XML Permissions • Place a new xml file in SYSVOL & set Everyone:Deny • Audit Access Denied errors. • Scan Active Directory Domains, OUs, AdminSDHolder, & GPOs for inappropriate custom permissions Credit: Rahmat Nurfauzi (https://github.com/infosecn1nja/AD-Attack-Defense/blob/master/ README.md#defense-evasion) Sean Metcalf (https://adsecurity.org/?p=2288)

- 26.

  Key Takeaways &Outlook • Automated Malware + Interactive Human Exploitation Operator -> New Cybercrime Frontier • Active Directory & Network Enumeration are the key to identify high-value corporate and multi-tenancy targets for additional monetization (e.g., Ryuk ransomware) • Cloud MSP are the desired targets as they are gateways to their customer environments (e.g., CloudJumper) Credit: CloudJumper image (https://www.drawingtutorials101.com/how-to-draw-cloudjumper-from-how-to-train-your-dragon-2)

- 27.
- 28.

  La Fin Thank youfor attending! Please feel free to reach out. @VK_Intel

---