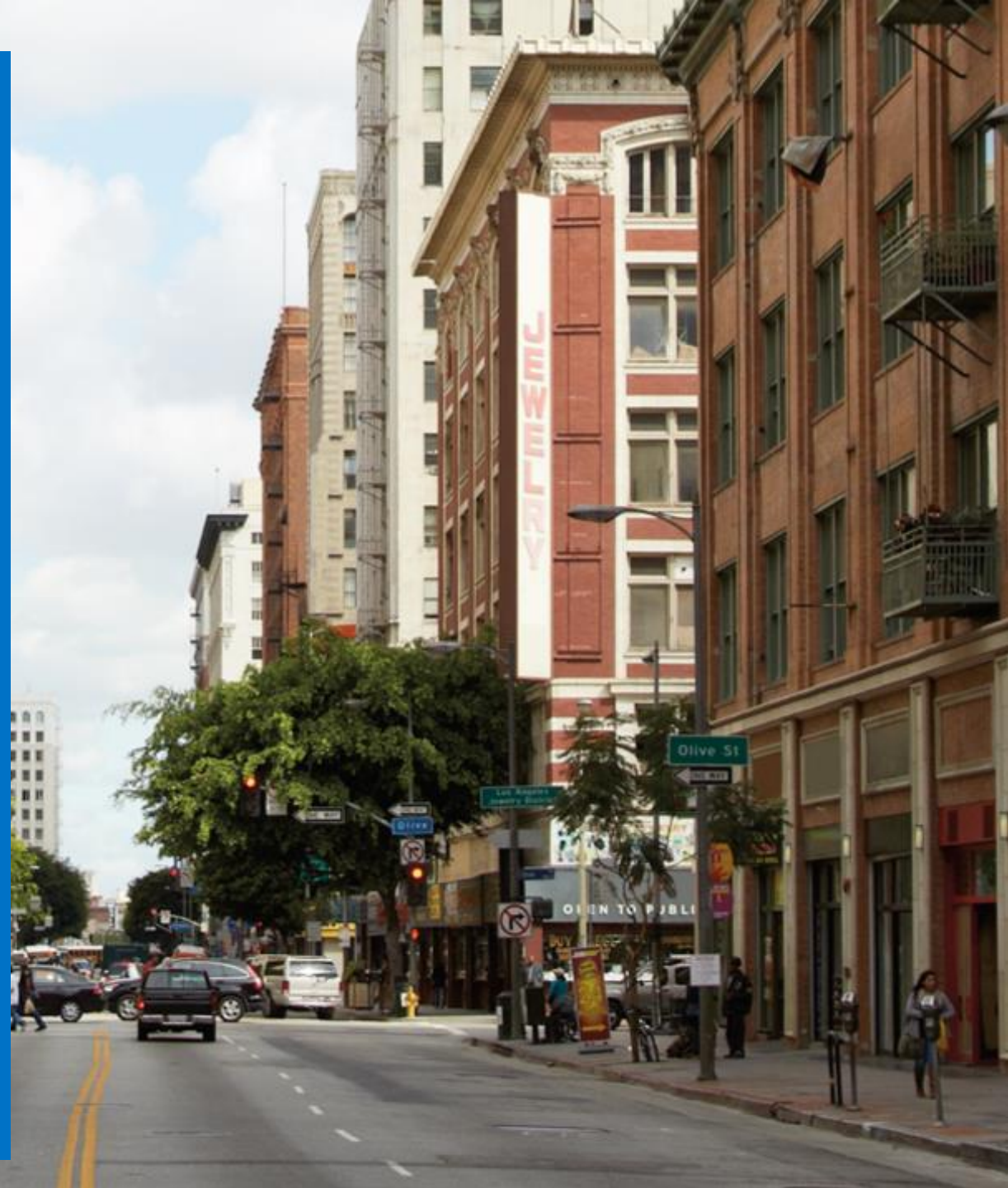




Microsoft Advanced Threat Analytics

Mgr. Michael Grafnetter

Architect



Agenda

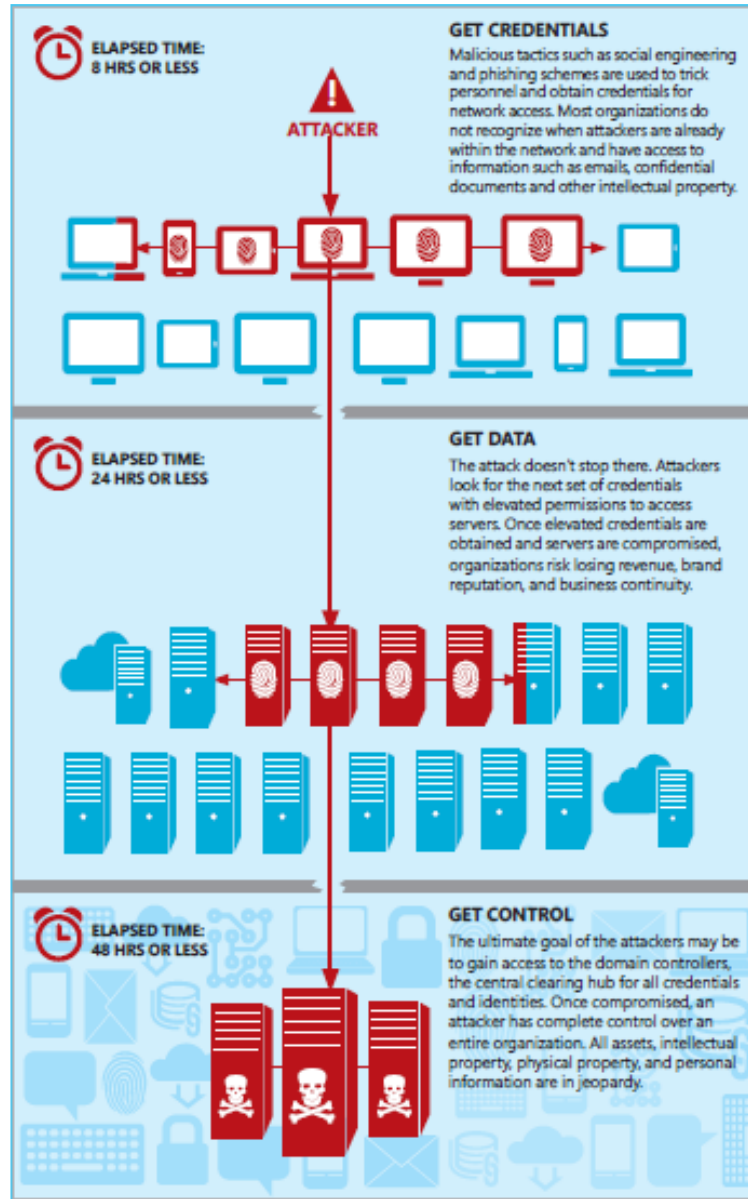
- ATA Overview
- ATA Deployment and Configuration
- Live Hacking Session



Advanced Infrastructure Attacks



Lateral Movement



Advanced Hacking Tools

The image shows a screenshot of the Cobalt Strike interface. The main window displays a network diagram with a central host labeled "67.180 root (0) @ Pineapple" at the top. Below it are two intermediate hosts: "172.16.42.1" and "172.16.42.42". The central host is connected to a series of target hosts at the bottom: "10.73.31.149", "10.73.31.186", "10.73.31.45", "10.73.31.40", "10.73.31.176", "10.73.31.6", "10.73.31.1", and "10.73.31.10". A terminal window at the bottom shows the following text:

```
02:44:59 [*] Meterpreter session 94 opened (10.195.21.54:8181 -> 67.180. . :48124) at
2012-06-14 02:44:59 +0000
02:46:17 * raffiz added pivot: 10.73.31.0 255.255.255.0 94
02:46:27 * raffiz ping sweep: 10.73.31.0/24 via 94
02:49:37 * raffiz launched msf scans at: 10.73.31.149, 10.73.31.186, 10.73.31.45, 10.73.31.40,
10.73.31.176, 10.73.31.6, 10.73.31.1, 10.73.31.10
02:56:30 <raffiz > we've pivoting through the wifi pineapple, which allowed us to get a
linux host, which allowed us to get java meterpreter on it, which allowed us to well... get
another network
02:56:31 <raffiz > cheers
02:57:47 <Darren > Way to go WiFi Pineapple / Cobalt Strike. Tasty fruit!
raffiz>
```

The terminal window also shows a "Current Call" notification for "Darren" at "01:38:41".

Motivated Hackers



Sobering Statistics

Common Cyber Attacks: Reducing The Impact

Most cyber attacks are composed of four stages: **Survey**, **Delivery**, **Breach** and **Affect**. The following **security controls**, applied at each stage of an attack, can reduce your organisation's exposure to a successful cyber attack.

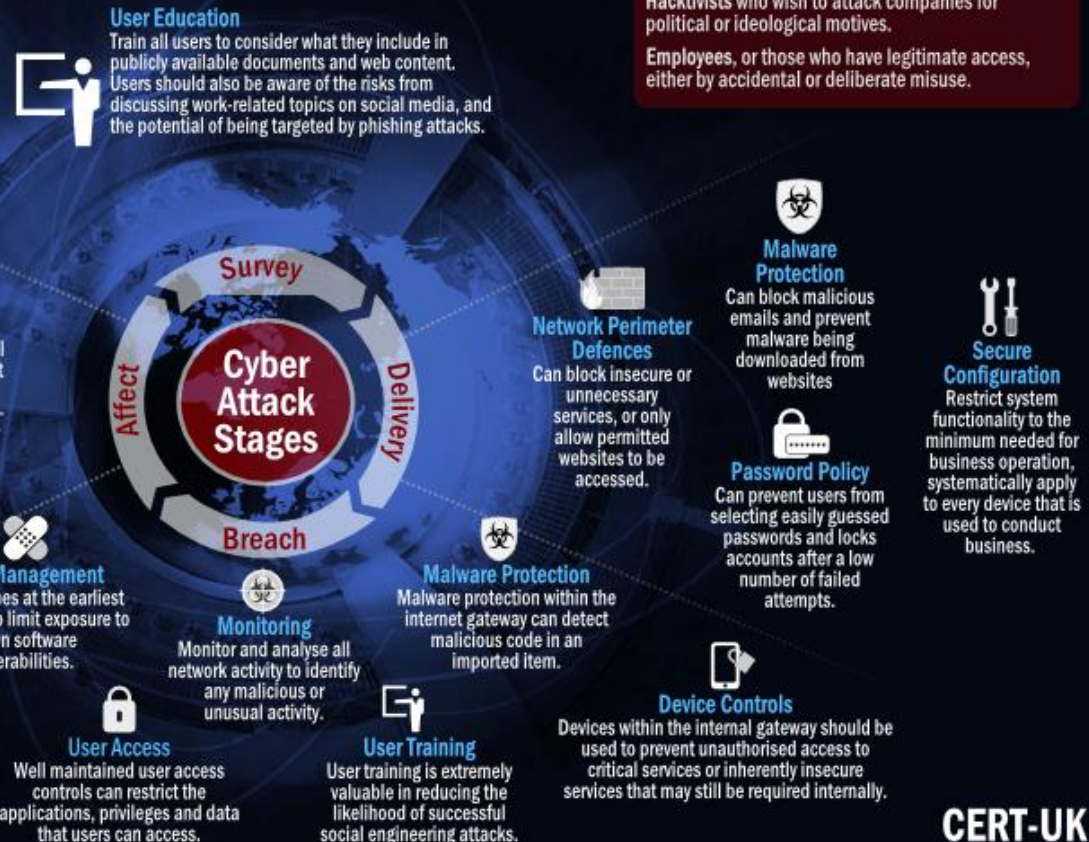
81%

OF LARGE COMPANIES
REPORTING BREACH

**£600K -
£1.15m**

AVERAGE COST OF
SECURITY BREACH

Source: 2014 Information
Security Breaches Survey
sponsored by the
Department for Business,
Innovation and Skills.



CERT-UK

Sobering Statistics

243

The average number of days that attackers reside within a victim's network before detection



76%

of all network intrusions are due to compromised user credentials



\$500B

The total potential cost of cybercrime to the global economy



\$3.5M

The average cost of a data breach to a company



The frequency and sophistication of cybersecurity attacks are getting worse.

The Problem

Traditional IT security tools are typically:

▶ Complex

Initial setup, fine-tuning, creating rules and thresholds/baselines can take a long time.

▶ Prone to false positives

You receive too many reports in a day with several false positives that require valuable time you don't have.

▶ Designed to protect the perimeter

When user credentials are stolen and attackers are in the network, your current defenses provide limited protection.



Advanced Threat Analytics Overview



Introducing Microsoft Advanced Threat Analytics

An on-premises platform to identify advanced security attacks *before* they cause damage



Behavioral
Analytics



Detection for known
attacks and issues



Advanced Threat
Detection

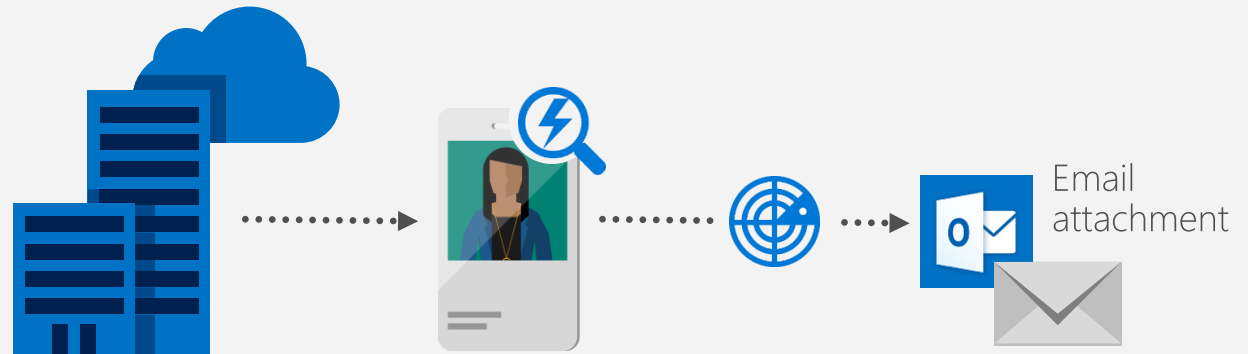
Introducing Microsoft Advanced Threat Analytics

An on-premises platform to identify advanced security attacks *before* they cause damage

Comparison:

- **Credit card** companies monitor cardholders' behavior.
- If there is any abnormal activity, they will notify the cardholder to verify charge.

Microsoft Advanced Threat Analytics brings this concept to IT and users of a particular organization



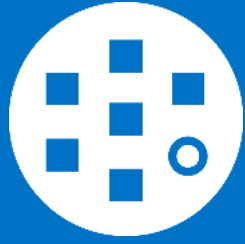
Why Microsoft Advanced Threat Analytics?



Speed

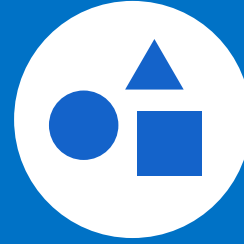
No need to create rules, thresholds, or baselines.

ATA detects suspicious activity fast, leveraging Active Directory traffic and SIEM logs.



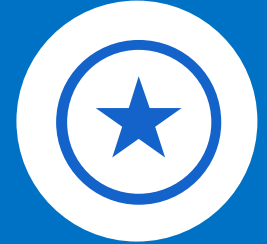
Adaptability

Self-learning behavioral analytics consistently learns and identifies abnormal behavior.



Simplicity

Functional, clear, and actionable attack timeline, showing the who, what, when, and how in near real time.

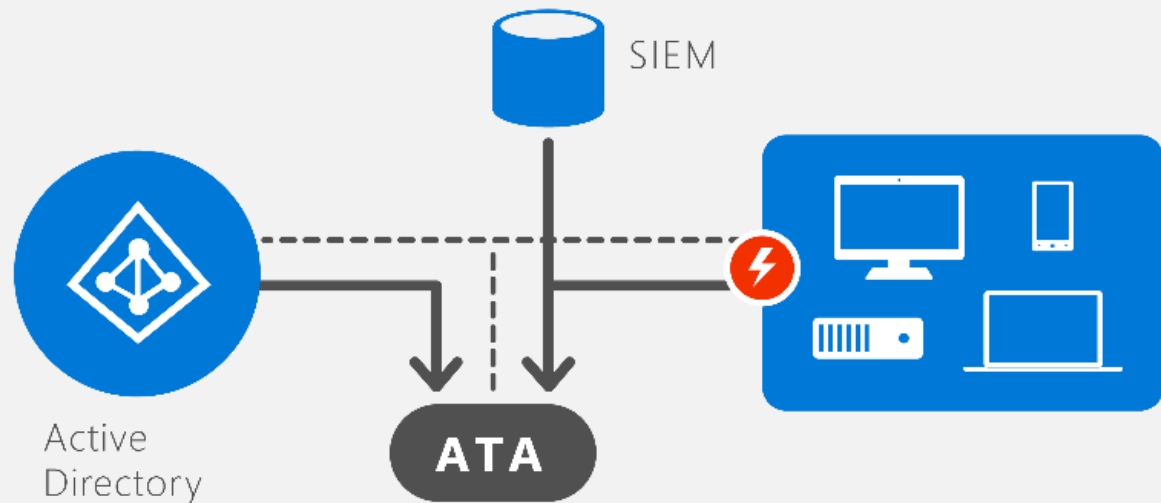


Accuracy

ATA compares the entity's behavior to its profile, but also to the other users, so red flags are raised only when verified.

How Microsoft Advanced Threat Analytics Works

1 Analyze

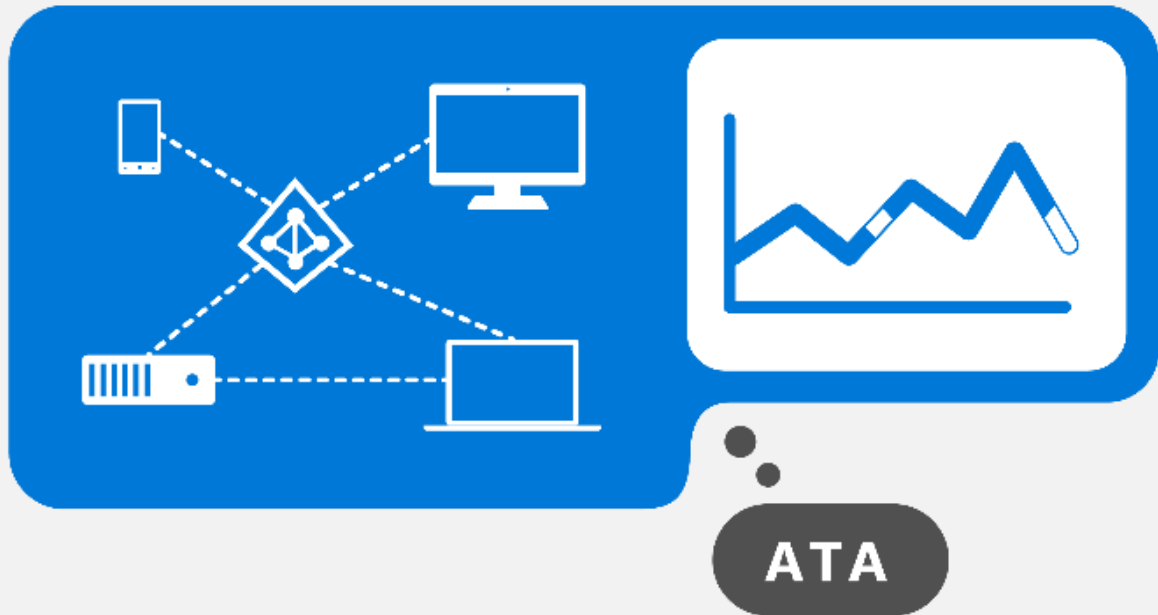


After installation:

- Simple non-intrusive port mirroring configuration copies all AD-related traffic
- Remains invisible to the attackers
- Analyzes all Active Directory traffic
- Collects relevant events from SIEM and other sources

How Microsoft Advanced Threat Analytics Works

2 Learn



ATA:

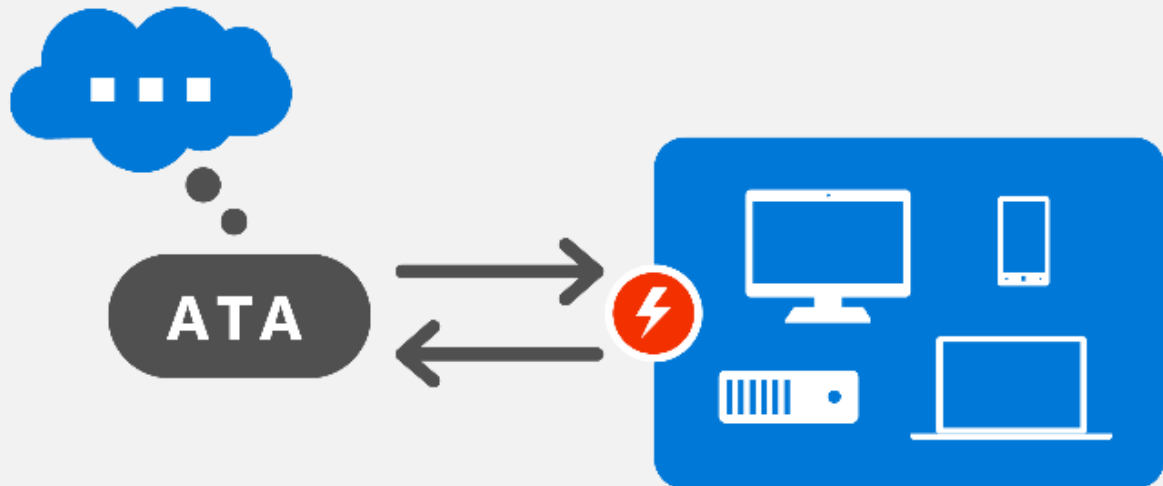
- Automatically starts learning and profiling entity behavior
- Identifies normal behavior for entities
- Learns continuously to update the activities of the users, devices, and resources

What is entity?

Entity represents users, devices, or resources

How Microsoft Advanced Threat Analytics Works

3 Detect



Microsoft Advanced Threat Analytics:

- Looks for abnormal behavior and identifies suspicious activities
- Only raises red flags if abnormal activities are contextually aggregated
- Leverages world-class security research to detect known attacks and security issues (regional or global)

ATA not only compares the entity's behavior to its own, but also to the behavior of entities in its interaction path.

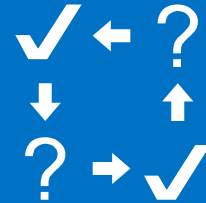
How Microsoft Advanced Threat Analytics Works

4 Alert

ATA reports all suspicious activities on a simple, functional, actionable attack timeline



ATA identifies
Who?
What?
When?
How?



For each suspicious activity, ATA provides recommendations for the investigation and remediation.



What ATA Detects

Abnormal resource access
Account enumeration
Net Session enumeration
DNS enumeration

Abnormal authentication
Abnormal resource access
Pass-the-Ticket
Pass-the-Hash
Overpass-the-Hash

Skeleton key malware
Golden ticket
Remote execution
Malicious replication requests

Compromised
Credential

Privilege
Escalation



Reconnaissance

Lateral
Movement

Domain
Dominance

Abnormal working hours
Brute force using NTLM, Kerberos or LDAP
Sensitive accounts exposed in plain text authentication
Service accounts exposed in plain text authentication
Honey Token account suspicious activities
Unusual protocol implementation
Malicious Data Protection Private Information (DPAPI) Request

MS14-068 exploit (Forged PAC)
MS11-013 exploit (Silver PAC)

What ATA Detects

Forbes / Opinion / #CyberSecurity

JUN 15, 2016 @ 12:44 AM

97,981 VIEWS

The Little Black Book of Billionaire Secrets

What Russia's DNC Hack Tells Us About Hillary Clinton's Private Email Server

CNN Money International +

Markets Economy Companies Tech

Iran hacked an American casino

Technet.cz

iDNES.cz > Zprávy | Kraje | Sport | Kultura | Ekonomika | Bydlení | Technet | Ona | Revue | Auto

Audio | Video | Tv | Foto | PC & Mac | Software | Notebooky | Web | Věda & Vesmír | Vojenství | Autoři



Zkusili jsme armádní brýle za 350 tisíc. Piloti mají nový simulátor tmy



Vzácné zeminy budeme možná těžit z mořského dna. Podíl na tom má CIA



Hackeri podleli útoku, unikly faktury a hesla. Kupovala i Policie ČR

theguardian

home > tech

UK world sport football opinion culture business lifestyle all

Hacking

US government hack stole fingerprints of 5.6 million federal employees

SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Subscribe (Free) | CISO Forum 2016

Malware & Threats Cybercrime Mobile & Wireless Risk & Compliance Security Architecture Manag

Home > Cybercrime



"FIN6" Cybergang Steals Millions of Cards From PoS Systems

ars technica

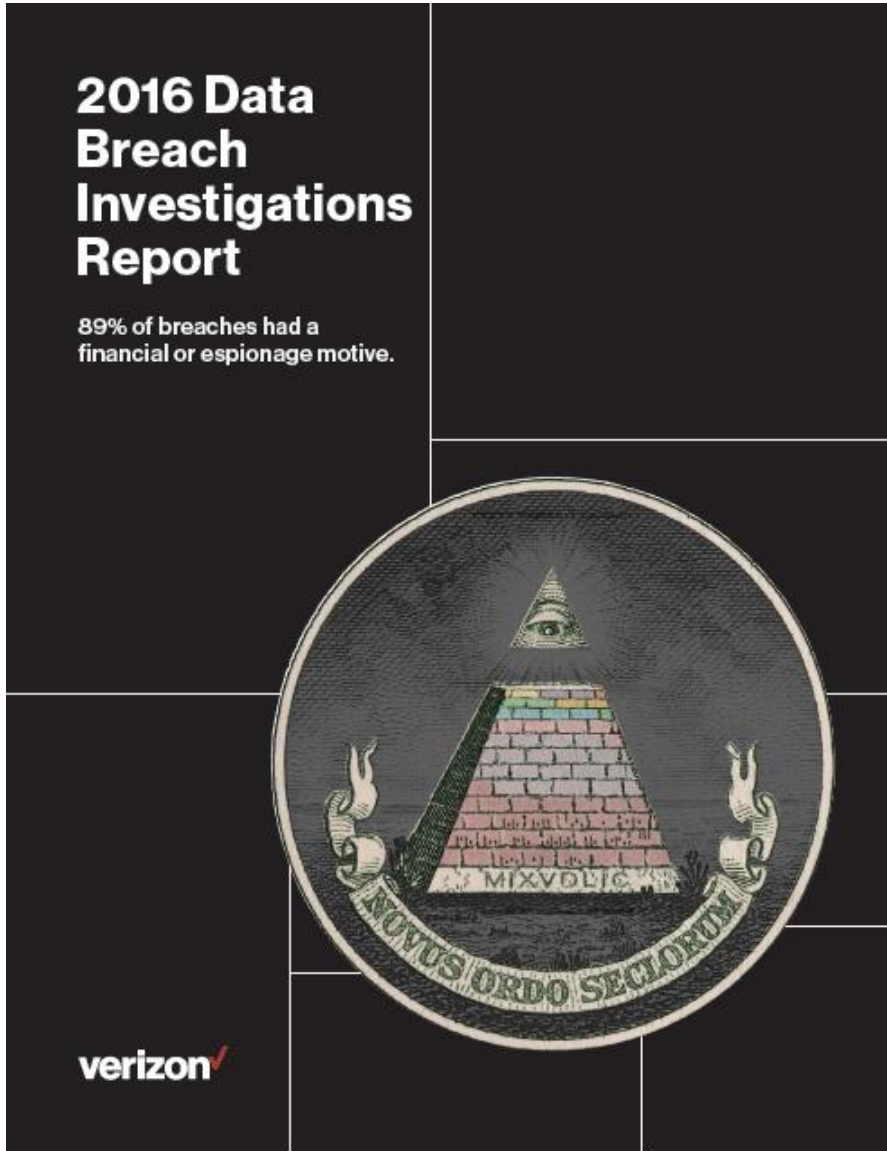
MAIN MENU MY STORIES: 25 FORUMS SUBSCRIBE JOBS

RISK ASSESSMENT / SECURITY & HACKTIVISM

How Hacking Team got hacked

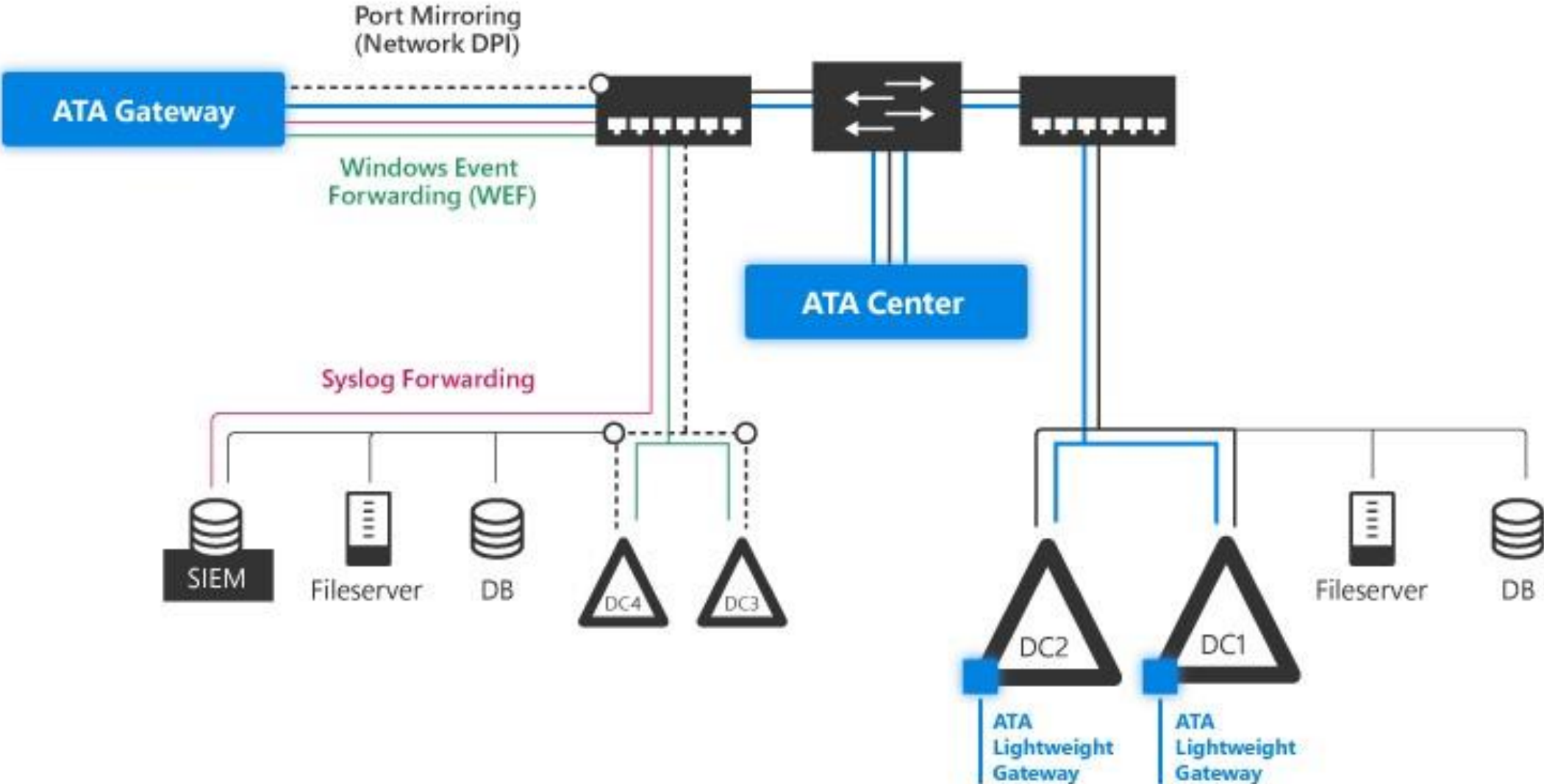
A black hat claims responsibility for the hack. Here's how he says he did it.

Really Popular Attack Vectors




63% of confirmed data breaches involved weak, default or stolen passwords.

ATA Architecture



Entity Views




Grafnetter Michael
Cloud and Security Advisor
External
mainstream.local
Created on Jan 26, 2016
+420 608075370 | Michael.Grafnetter@mainstream.cz

About Account Info Suspicious activities Directory Changes

Memberships (12)

- PSLAB_TG
- Mainstream-All
- TG_Access
- Domain Users
All domain users
- Mainstream Team
- Cloud Team

Password



MAIN024NB
Windows 10 Enterprise, 10.0 (10586)
mainstream.local
Created on Jan 28, 2016

About Account Info Suspicious activities Directory Changes

Memberships (1)

- Domain Computers
All workstations and servers joined to the domain

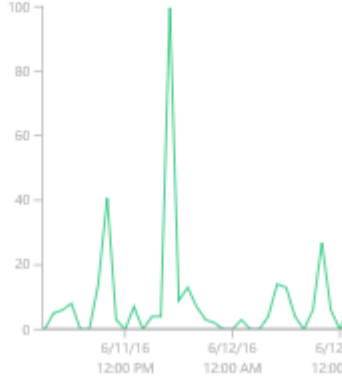
Password

Last change
Monday, May 30, 2016 at 8:37 AM

Sites

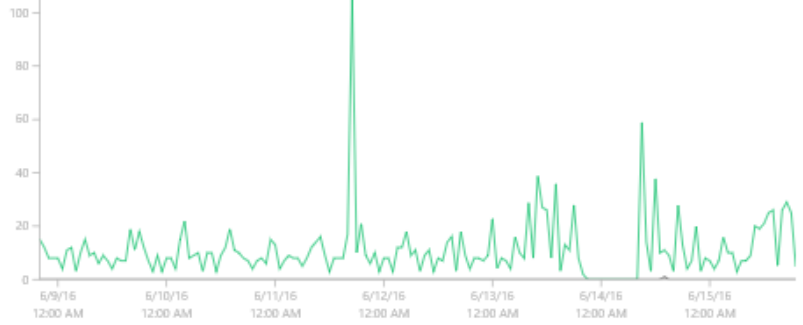
- Hvezdova
172.27.126.179
Last seen
Wednesday, June 15, 2016 at 7:30 PM
- 172.27.126.109
Last seen
Tuesday, June 14, 2016 at 9:09 AM
- 172.27.126.103
Last seen
Tuesday, May 31, 2016 at 9:08 AM

User activity




Computer activity


● Kerberos ● NTLM



Users who recently logged onto this computer

-  Grafnetter Michael
Cloud and Security Advisor
Wednesday, June 15, 2016 at 6:32 PM

Recently accessed resources

-  MAINSTREAM.LOCAL
to KRBTGT
Wednesday, June 15, 2016 at 7:30 PM

Detailed Excel Exports

Suspicion of identity theft based on abnormal behavior 57614fef393ec816c02c825a.xls...

FILE HOME INSERT PAGE LAYOUT FORMULAS DATA REVIEW VIEW ADD-INS OFFICE REMOTE TEAM DESIGN Michael G...

A841 : X ✓ fx 5/12/2016 1:01:00

| | Time (UTC) | Source Ip Address | Source Port | Destination Ip Address | Destination Port | Transport Protocol | Type |
|-----|--------------------------|-------------------|-------------|------------------------|------------------|--------------------|------------|
| 841 | 5/12/2016 1:01:00.480 AM | 192.168.110.11 | 43392 | 172.27.126.10 | 88 | Tcp | KerberosAs |
| 842 | 5/12/2016 1:01:09.528 AM | 192.168.110.11 | 43418 | 172.27.126.10 | 88 | Tcp | KerberosAs |
| 843 | 5/12/2016 1:01:09.532 AM | 192.168.110.11 | 43419 | 172.27.126.10 | 88 | Tcp | KerberosAs |
| 844 | 5/12/2016 1:01:12.762 AM | 192.168.110.11 | 43428 | 172.27.126.10 | 88 | Tcp | KerberosAs |
| 845 | 5/12/2016 1:01:12.769 AM | 192.168.110.11 | 43429 | 172.27.126.10 | 88 | Tcp | KerberosAs |
| 846 | 5/12/2016 1:01:13.003 AM | 192.168.110.11 | 43431 | 172.27.126.10 | 88 | Tcp | KerberosAs |
| 847 | 5/12/2016 1:01:13.013 AM | 192.168.110.11 | 43432 | 172.27.126.10 | 88 | Tcp | KerberosAs |
| 848 | 5/12/2016 1:01:16.546 AM | 192.168.110.11 | 43452 | 172.27.126.10 | 88 | Tcp | KerberosAs |

Summary | Source Account | Normal Source Computers ...

READY 70%

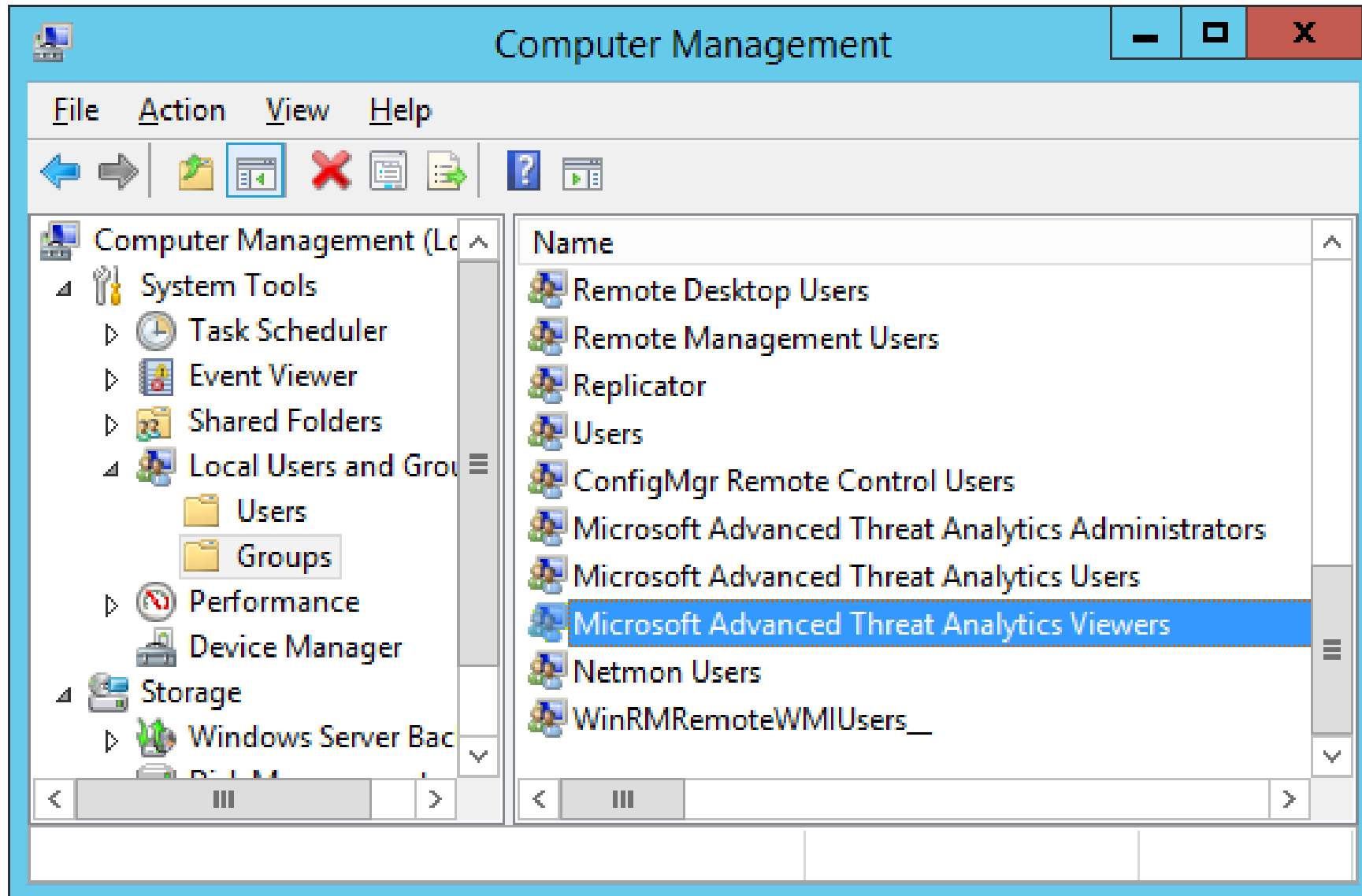
Demo 



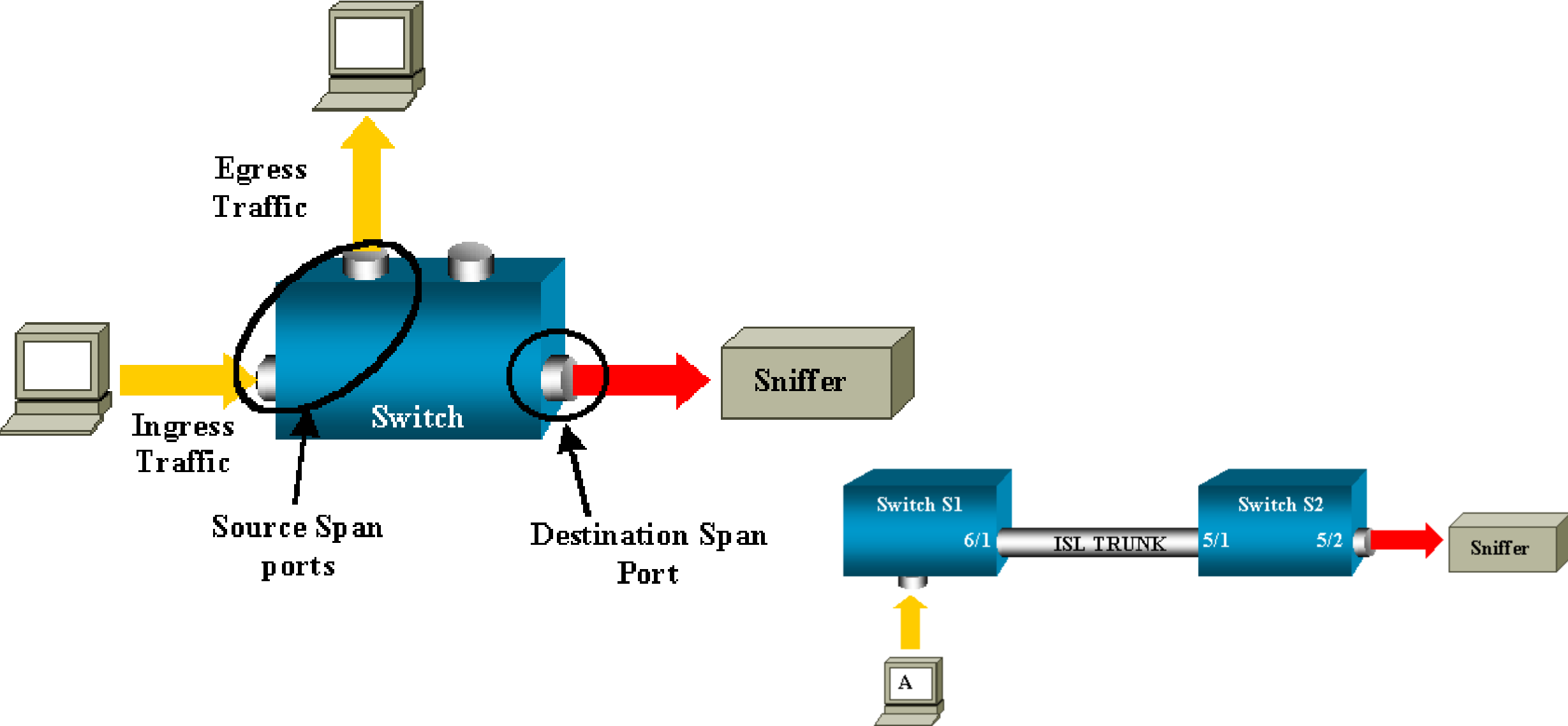
ATA Deployment and Configuration



ATA Center RBAC



Configuration – ATA Gateway



Configuration – ATA Gateway – Hyper-V

The image shows the configuration interface for a Hyper-V virtual machine. The left pane displays the 'Advanced Features' section, with 'Management' expanded. The right pane shows various network-related settings, with the 'Port mirroring' section highlighted by a red border.

Advanced Features

- Hardware Acceleration
- Advanced Features**
- Management**
- Name: savdalata01
- Integration Services: Some services offered
- Checkpoint File Location: C:\Virtuals\savdalata01\savdalata01
- Smart Paging File Location: C:\Virtuals\savdalata01\savdalata01
- Automatic Start Action: Restart if previously running
- Automatic Stop Action: Save

Port mirroring

Port mirroring allows the network traffic of a virtual machine to be monitored by copying incoming and outgoing packets and forwarding the copies to another virtual machine configured for monitoring.

Mirroring mode: Destination

Configuration – ATA Gateway - Cisco

The screenshot displays the Cisco Smartports configuration interface. The main window is titled "Smartports" and has a "Port Setup" tab selected. It shows a virtual switch with 16 ports arranged in two rows. The top row ports are labeled 1x through 16x, and the bottom row ports are labeled 2x through 16x. A yellow box highlights port 13x in the top row. A "PoE" label is visible below the first two ports of the bottom row. To the right, a "0-24LC" module is partially visible.

A "Modify Port Roles" dialog box is open over the switch. It contains the following fields and controls:

- Interface:** FastEthernet13
- Role:** Diagnostics (selected from a dropdown menu)
- Attributes:**
 - Source Port:** FastEthernet3 (selected from a dropdown menu)
 - Ingress VLAN:** default (1) (selected from a dropdown menu)
- Buttons:** OK, Cancel, Help
- Original value:** none

At the bottom of the main window, there are two rows of buttons: "Suggest", "Modify", "Details" and "OK", "Apply", "Refresh", "Cancel", "Help".

Configuration - Detection


ATA Gateways

ATA Center

Detection

Alerts

Licensing

 **Detection**

Short-term lease subnets [?]

Honeytoken account SIDs

DNS Reconnaissance IP address exclusions

Pass-the-Ticket IP address exclusions

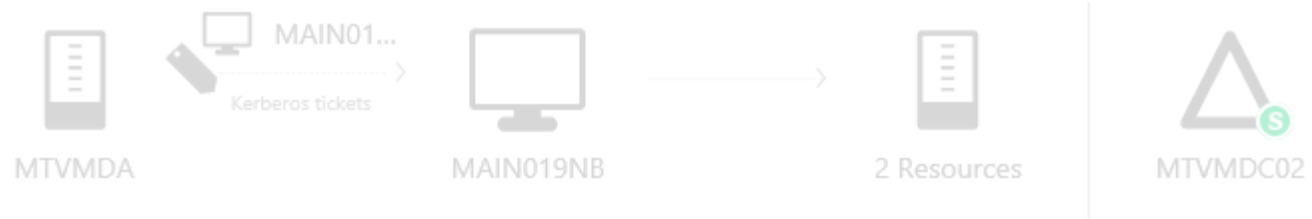
Exceptions for NAT, DA and AADSync

Identity Theft Using Pass-the-Ticket Attack

MAIN019NB's Kerberos tickets were stolen from MTVMDA to MAIN019NB and used to access 2 resources.

Note Email Export to Excel Details Input Open

Are any of these computers NAT devices, DirectAccess servers or computers connecting via NAT or DirectAccess?



Computers (2)

- MAIN019NB No Yes
- MTVMDA No Yes

Save

Cancel

Resolved vs. Dismissed

Suspicion of identity theft based on abnormal behavior ?

MTVMEX03 exhibited abnormal behavior when performing activities that were not seen over the last month and are also not in accordance with the activities of other accounts in the organization. The abnormal behavior is based on the following activities:

- Requested access to 3 abnormal resources.

5/25/16 4:16 PM > 4:40 PM

Summary Details Note Share Export to Excel Input Open

Resolved

Dismissed

MTVMEX03 Accessed 31 normal resources + 3 abnormal resources

Note



Suspicion of identity theft based on abnormal behavior ?

MTVMEX03 exhibited abnormal behavior when performing activities that were not seen over the last month and are also not in accordance with the activities of other accounts in the organization. The abnormal behavior is based on the following activities:

- Requested access to 3 abnormal resources.

5/25/16 4:16 PM > 4:40 PM

Summary

Details

 Note

 Share

 Export to Excel

Input

Open

Type your note here

Save

Cancel

MongoDB

The screenshot displays the MongoBooster application window. The title bar reads "MongoBooster". The menu bar includes "File", "Edit", "Options", "View", "Window", and "Help". The toolbar contains icons for "Connect", "Open", "Save", "Import", "Export", "Run", and "Stop".

The "Connection Tree" on the left shows a "New Connection" folder containing an "ATA" folder. Under "ATA", there are several collections, including "AccountBruteForceRecords (1)", "DirectoryServicesActivities (503)", and multiple "KerberosAps_" and "KerberosKdcs_" collections with varying document counts.

The main workspace shows a query executed against the "ATA" database on "localhost:27017 (v3.0.5)". The query is: `db.NtlmEvents_20160224.find({'SourceAccountName': 'mgrafnetter'})`. The result is displayed in a table view for the "NtlmEvents_20160224" collection, showing 649 documents in 60 ms.

| Key | Value | Type |
|--|--------------------------------------|----------|
| <input type="checkbox"/> IsTimeMilliseconds | true | Bool |
| <input type="checkbox"/> ProviderName | Microsoft-Windows-Security-Auditing | String |
| <input type="checkbox"/> SourceAccountId | 532f955b-6215-443d-a148-4be4153a3f8f | String |
| <input type="checkbox"/> SourceAccountName | mgrafnetter | String |
| <input type="checkbox"/> SourceComputerId | 3fe6f974-5664-4927-aa4e-80f9d8ec7e74 | String |
| <input checked="" type="checkbox"/> SourceComputerName | { 2 fields } | Object |
| <input type="checkbox"/> DomainName | null | Null |
| <input type="checkbox"/> Name | MAIN024NB | String |
| <input type="checkbox"/> Time | 2/24/2016, 2:15:34 AM | Date |
| <input type="checkbox"/> (16) ObjectId("56cd08f...") | { 13 fields } | Document |

At the bottom of the window, the status bar shows: "Copyright© mongo booster.com version 1.3.2 Paid for features, 21 days left", "Feedback/Support", "Show Log", and the time "04:28:35 pm".

Integration - SIEM

- Splunk
- HP Arcsight
- RSA Security Analytics
- IBM QRadar
- ...

Integration - Syslog

Syslog



Syslog server endpoint

nagios.mainstream.local

:

514

Transport

UDP



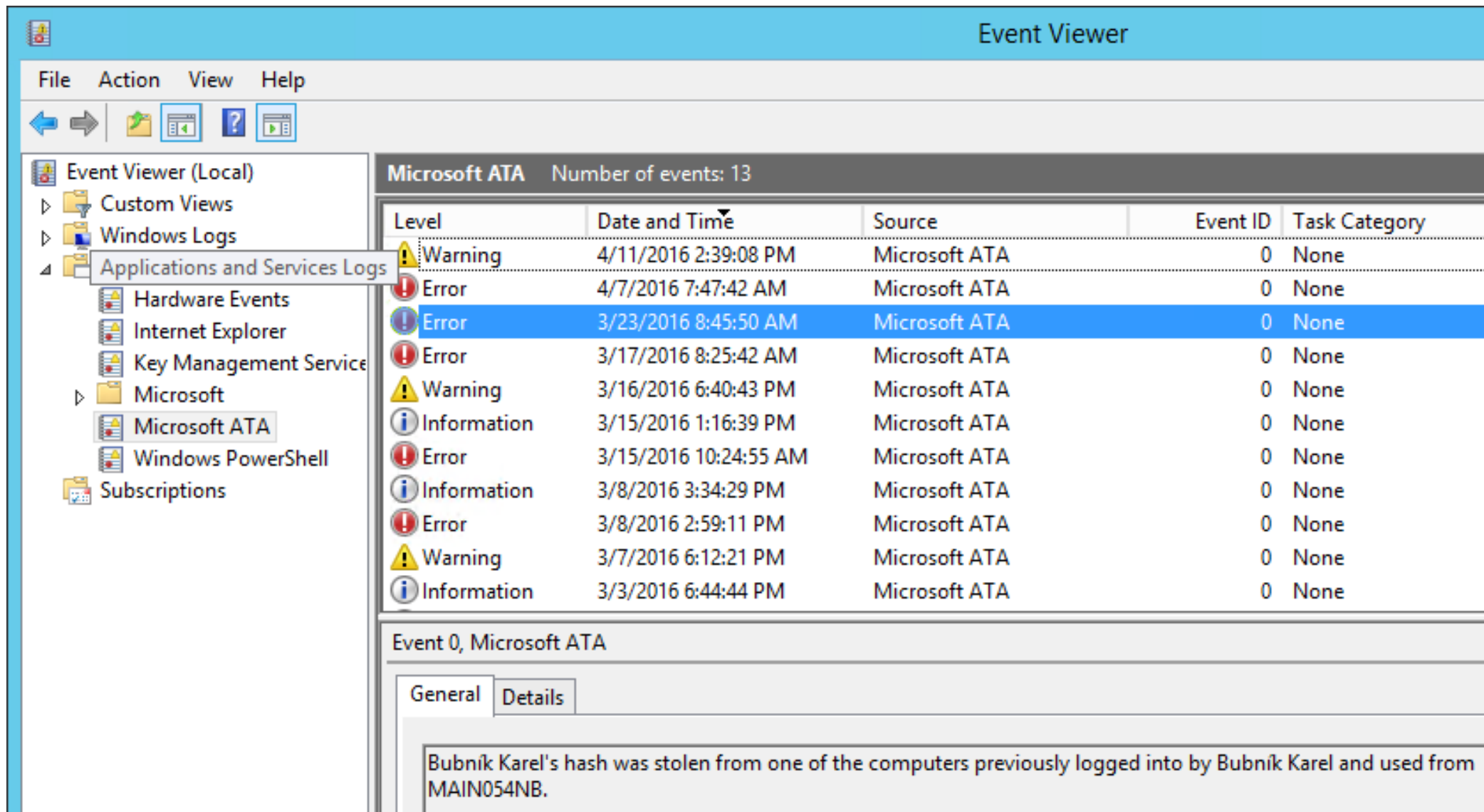
Format

RFC 5424



RFC 3164

Integration - SCOM



Event Viewer

File Action View Help

Event Viewer (Local)

- Custom Views
- Windows Logs
- Applications and Services Logs
 - Hardware Events
 - Internet Explorer
 - Key Management Service
 - Microsoft
 - Microsoft ATA
 - Windows PowerShell
- Subscriptions

Microsoft ATA Number of events: 13

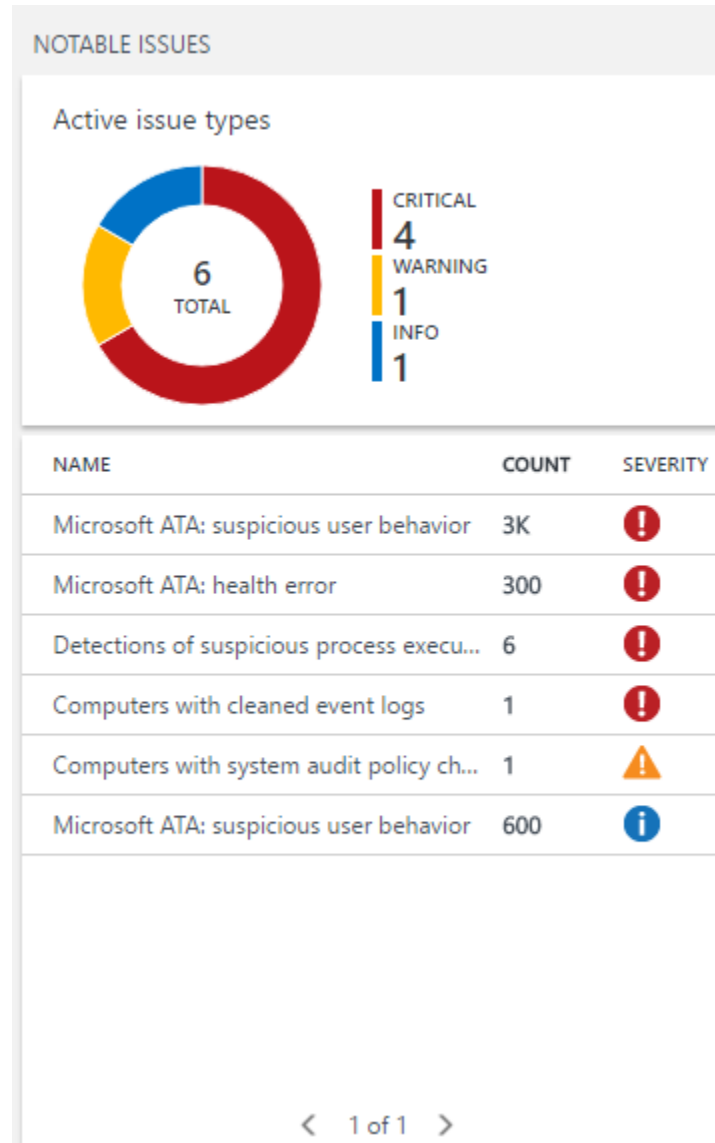
| Level | Date and Time | Source | Event ID | Task Category |
|-------------|-----------------------|---------------|----------|---------------|
| Warning | 4/11/2016 2:39:08 PM | Microsoft ATA | 0 | None |
| Error | 4/7/2016 7:47:42 AM | Microsoft ATA | 0 | None |
| Error | 3/23/2016 8:45:50 AM | Microsoft ATA | 0 | None |
| Error | 3/17/2016 8:25:42 AM | Microsoft ATA | 0 | None |
| Warning | 3/16/2016 6:40:43 PM | Microsoft ATA | 0 | None |
| Information | 3/15/2016 1:16:39 PM | Microsoft ATA | 0 | None |
| Error | 3/15/2016 10:24:55 AM | Microsoft ATA | 0 | None |
| Information | 3/8/2016 3:34:29 PM | Microsoft ATA | 0 | None |
| Error | 3/8/2016 2:59:11 PM | Microsoft ATA | 0 | None |
| Warning | 3/7/2016 6:12:21 PM | Microsoft ATA | 0 | None |
| Information | 3/3/2016 6:44:44 PM | Microsoft ATA | 0 | None |

Event 0, Microsoft ATA

General Details

Bubník Karel's hash was stolen from one of the computers previously logged into by Bubník Karel and used from MAIN054NB.

Integration – Azure OMS



Integration – Azure OMS

Microsoft Operations Management Suite

Search

Export Alert Save Favorites History

Data based on last 7 days

1 bar = 6 hrs

TYPE (1)

| | |
|-------------------|----|
| SecurityDetection | 2K |
|-------------------|----|

COMPUTER (1)

| | |
|----------------|----|
| OrcoOMSProdPub | 2K |
|----------------|----|

ALERTSEVERITY (2)

| | |
|------|-----|
| high | 2K |
| low | 394 |

ALERTTITLE (2)

| | |
|---------------------|-----|
| Suspicious Activity | 2K |
| Health | 197 |

Type:SecurityDetection

2K Results List Table

5/25/2016 10:43:58.000 AM | SecurityDetection

- TimeGenerated : 5/25/2016 10:43:58.000 AM
- Computer : OrcoOMSProdPub
- AlertSeverity : High
- Description : Administrator successfully authenticated from CLIENT23 against DC1 using an unusual protocol implementation. This may t
- AlertTitle : Suspicious Activity
- SourceSystem : OpsManager
- Provider : Microsoft ATA
- OriginalSeverity : 2

[-] show less

5/25/2016 10:43:58.000 AM | SecurityDetection

- TimeGenerated : 5/25/2016 10:43:58.000 AM
- Computer : OrcoOMSProdPub
- AlertSeverity : High
- Description : SMB session enumeration attempts failed from CLIENT23 against DC1. No accounts were exposed.
- AlertTitle : Suspicious Activity

[+] show more

5/25/2016 10:43:58.000 AM | SecurityDetection

- TimeGenerated : 5/25/2016 10:43:58.000 AM
- Computer : OrcoOMSProdPub
- AlertSeverity : Low
- Description : The following remote execution attempts were performed on DC1 from CLIENT1: Successful remote creation of FcgYYgni.
- AlertTitle : Suspicious Activity

[+] show more

Updates through MS Update / WSUS

Microsoft Advanced Threat Analytics — X

Use Microsoft Update to help keep your computer secure and up-to-date

↓ Microsoft Update offers security and important updates for Windows and other Microsoft products, including Microsoft Advanced Threat Analytics. Updates are delivered using your Automatic Updates settings, or you can visit the Microsoft Update Web site.

Use Microsoft Update when I check for update (recommended)

I don't want to use Microsoft Update

[See the Microsoft Update FAQ](#)
[Read our Privacy Statement online](#)

Back **Next**

Capacity Planning – ATA Center

| PACKETS PER SECOND* | CPU (CORES**) | MEMORY (GB) | DATABASE STORAGE PER DAY (GB) | DATABASE STORAGE PER MONTH (GB) | IOPS*** |
|----------------------------|----------------------|--------------------|--------------------------------------|--|----------------|
| 1,000 | 2 | 32 | 0.3 | 9 | 30 (100) |
| 10,000 | 4 | 48 | 3 | 90 | 200 (300) |
| 40,000 | 8 | 64 | 12 | 360 | 500 (1,000) |
| 100,000 | 12 | 96 | 30 | 900 | 1,000 (1,500) |
| 400,000 | 40 | 128 | 120 | 1,800 | 2,000 (2,500) |

Capacity Planning - ATA Lightweight GW

| PACKETS PER SECOND* | CPU (CORES**) | MEMORY (GB)*** |
|----------------------------|----------------------|-----------------------|
| 1,000 | 2 | 6 |
| 5,000 | 6 | 16 |
| 10,000 | 10 | 24 |

Capacity Planning – ATA Gateway

| PACKETS PER SECOND* | CPU (CORES**) | MEMORY (GB) |
|----------------------------|----------------------|--------------------|
| 1,000 | 1 | 6 |
| 5,000 | 2 | 10 |
| 10,000 | 3 | 12 |
| 20,000 | 6 | 24 |
| 50,000 | 16 | 48 |

Capacity Planning – ATA Gateway

Dropped port mirrored network traffic

ATA Gateway, CZES000ATAG001, is receiving more network traffic than it can process. A portion of the network traffic is being dropped.

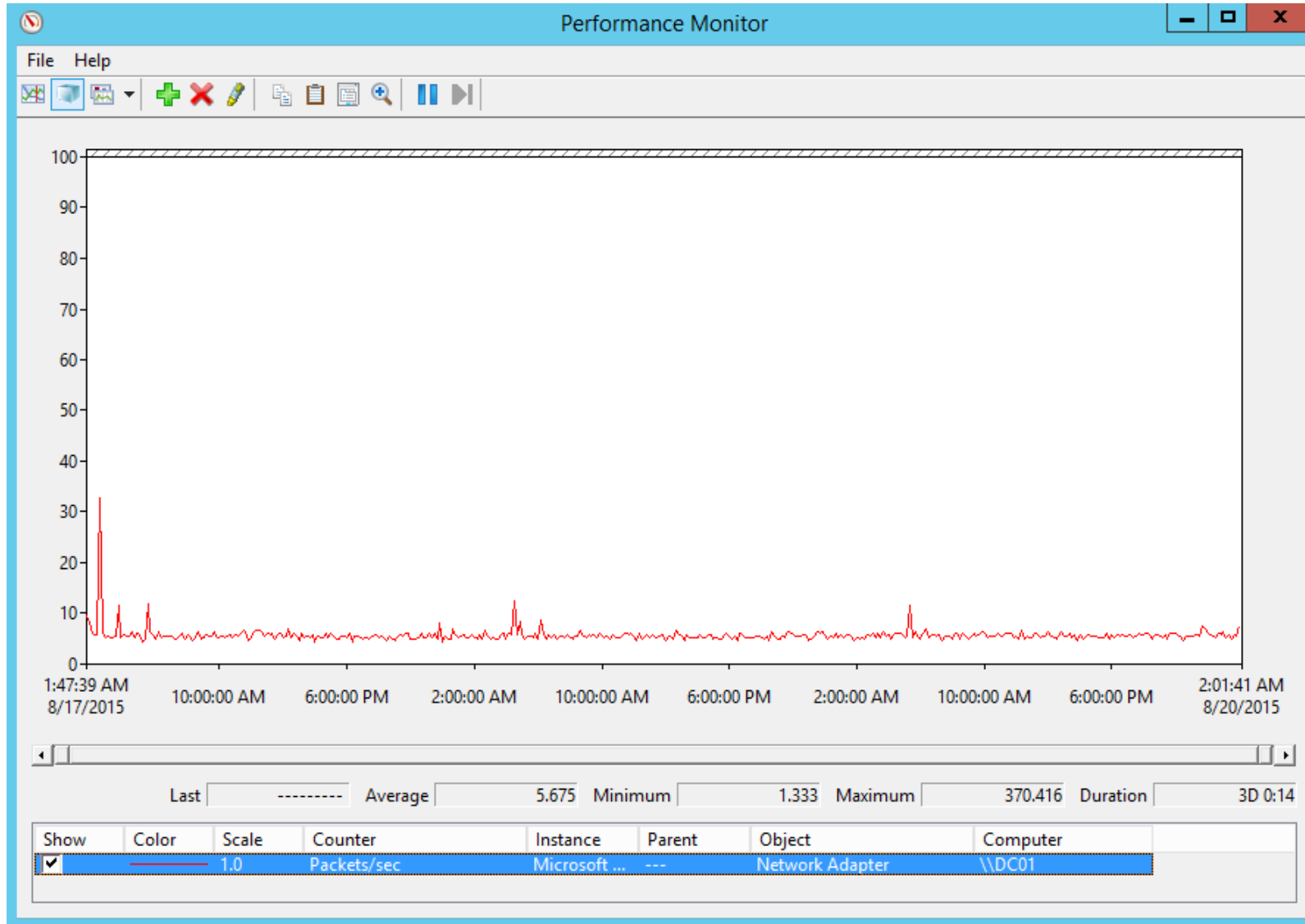
5/9/16 10:05 PM > 5/11/16 8:20 PM

 Resolved

Recommendations

- Consider adding additional processors and memory to the ATA Gateway or reducing the number of domain controllers being monitored by the ATA Gateway.

Capacity Planning – DC Monitoring



Capacity Planning – DC Monitoring

The screenshot shows the Windows Performance Monitor application. The left-hand tree view is expanded to 'Performance > Monitoring Tools > Performance Monitor > Data Collector Sets > User Defined > Packet...'. A context menu is open over the 'Packet...' item, listing the following actions: Start, Stop, Save Template..., Data Manager..., Latest Report, New, View, New Window from Here, Refresh, Export List..., Properties, and Help.

| Name | Type | Output |
|-----------------|---------------------|--|
| DataCollector01 | Performance Counter | C:\PerfLogs\Admin\Packets per second\DC01_20150817-000002\DataC... |

Monitoring ATA Health

ATA Gateway stopped communicating

There has not been communication from the ATA Gateway CZES000ATAG001 for at least 15 minutes. Last communication was on Monday, May 9, 2016 at 10:08 PM.

5/9/16 10:23 PM > 10:25 PM

 Resolved

Recommendations

- Check that the ATA Gateway service is up and running.
- Check the network connectivity between the ATA Gateway and the ATA Center Service.
- Check that the port used for the communication between the ATA Gateway and ATA Center Service is not blocked by any routers or firewalls.

ATA Center service is down

ATA Center service on CZES000ATAC001, has been down for at least 5 minutes. It was last seen running on Sunday, May 8, 2016 at 5:13 PM

5/8/16 5:19 PM > 5:52 PM

 Resolved

Recommendations

- Verify that the ATA Center service is running.
- Refer to the ATA Center logs to troubleshoot.

Monitoring ATA Performance

The screenshot displays the Windows Performance Monitor application. The left-hand navigation pane shows a tree view under 'Performance' with the following structure:

- Monitoring Tools
 - Performance Monitor
- Data Collector Sets
 - User Defined
 - Microsoft ATA Center
 - Server Manager Performance
- System
 - System Diagnostics
 - System Performance
- Event Trace Sessions
 - Event Trace Sessions
 - Startup Event Trace Sessions
- Reports
 - User Defined
 - System

The right-hand pane shows a table with the following content:

| Name | Type |
|----------------------|---------------------|
| Performance Counters | Performance Counter |

Below the table, the 'Performance Counters Properties' dialog is open, showing a list of performance counters. The selected counter is:

- Microsoft ATA Center (*) *

Other visible counters in the list include:

- Microsoft ATA Console (*) *
- \.NET Driver for MongoDB (*) *
- \.NET CLR Exceptions(Microsoft.Tri.Center)\# of...
- \.NET CLR Exceptions(Microsoft.Tri.Center)\# of...
- \.NET CLR LocksAndThreads(Microsoft.Tri.Cente...
- \.NET CLR LocksAndThreads(Microsoft.Tri.Cente...
- \.NET CLR LocksAndThreads(Microsoft.Tri.Cente...

Monitoring ATA Performance

Microsoft ATA Center

nt authority\system\microsoft.tri.center.exe

| | |
|--|--------|
| AppDomainManager UpdateExceptionStatistics Time | 0.000 |
| CenterConfigurationManager UpdateConfiguration Time | 66.000 |
| CenterDatabaseClient BackupSystemProfiles Time | 28.000 |
| CenterDatabaseClient DeleteOldCollections Time | 28.000 |
| CenterDatabaseClient DirectoryServicesActivities Block Input Items/Sec | 0.000 |
| CenterDatabaseClient DirectoryServicesActivities Block Output Batch Size | 1.000 |
| CenterDatabaseClient DirectoryServicesActivities Block Output Items/Sec | 0.000 |
| CenterDatabaseClient DirectoryServicesActivities Block Size | 0.000 |
| CenterDatabaseClient DirectoryServicesActivities Block Time | 2.000 |
| CenterDatabaseClient Dnss Block Input Items/Sec | 0.000 |
| CenterDatabaseClient Dnss Block Output Batch Size | 1.000 |
| CenterDatabaseClient Dnss Block Output Items/Sec | 0.000 |
| CenterDatabaseClient Dnss Block Size | 0.000 |
| CenterDatabaseClient Dnss Block Time | 39.000 |
| CenterDatabaseClient KerberosAps Block Input Items/Sec | 0.000 |
| CenterDatabaseClient KerberosAps Block Output Batch Size | 1.000 |



Live Hacking Session



DNS Reconnaissance

```
Command Prompt - nslookup - 192.168.110.31

> ls mainstream.cz
[mtvmdc02.mainstream.local]
mainstream.cz.      NS      serv[REDACTED]01.mainstream.local
mainstream.cz.      NS      serv[REDACTED]c01.mainstream.local
mainstream.cz.      NS      serv[REDACTED]03.mainstream.local
mainstream.cz.      NS      serv[REDACTED]02.mainstream.local
admin               A      192.168.110.10
autodiscover        A      192.168.110.10
cloud               A      192.168.110.10
ctx                 A      192.168.110.10
da                  A      192.168.110.10
directaccess        A      193.168.110.10
fs                  A      10.0.0.10
helpdesk            A      192.168.110.10
im                  A      172.16.110.10
intranet            A      172.16.110.10
jira                A      192.168.110.10
```

DNS Reconnaissance

Reconnaissance Using DNS

Suspicious DNS activity was observed, originating from NINJA (which is not a DNS server) against MTVMDC02.

 Note  Email  Export to Excel  Details  Input

 Open



NINJA

DNS queries



MTVMDC02

Recommendations

- Disconnect NINJA from the network, or move it into an isolated environment and start a forensics procedure by investigating: unknown processes, services, registry entries, unsigned files, and more
- Disable NINJA's account

Demo 

SMB Session Enumeration

Reconnaissance using SMB Session Enumeration

SMB session enumeration attempts were successfully performed from USER1-PC against DC1, exposing 4 accounts.

Note Share Export to Excel Details Input

Open



USER1-PC

Session Enumeration



DC1

Exposed Accounts (4)

SECRETS-DBS
on 192.168.0.210

user1
on 192.168.0.1

APP2S
on 192.168.0.5

user2
on 192.168.0.5

Recommendations

- Disconnect USER1-PC from the network, or move it into an isolated environment and start a forensics procedure by investigating: unknown processes, services, registry entries, unsigned files, and more.
- Verify that all enumerated accounts use a strong password.

SAM-R Enumeration

Reconnaissance using directory services enumeration

The following directory services enumerations using SAMR protocol were attempted against MTVMDC01 from MAIN024NB:

- Successful enumeration of all groups in mainstream.local by 2 accounts
- Successful enumeration of all users in mainstream.local by 2 accounts

Note Share Export to Excel Details Input

Open



2 accounts

On



MAIN024NB

Directory Services Enumeration



MTVMDC01

Operations (2)



Enumerate all groups
in mainstream.local



Enumerate all users
in mainstream.local

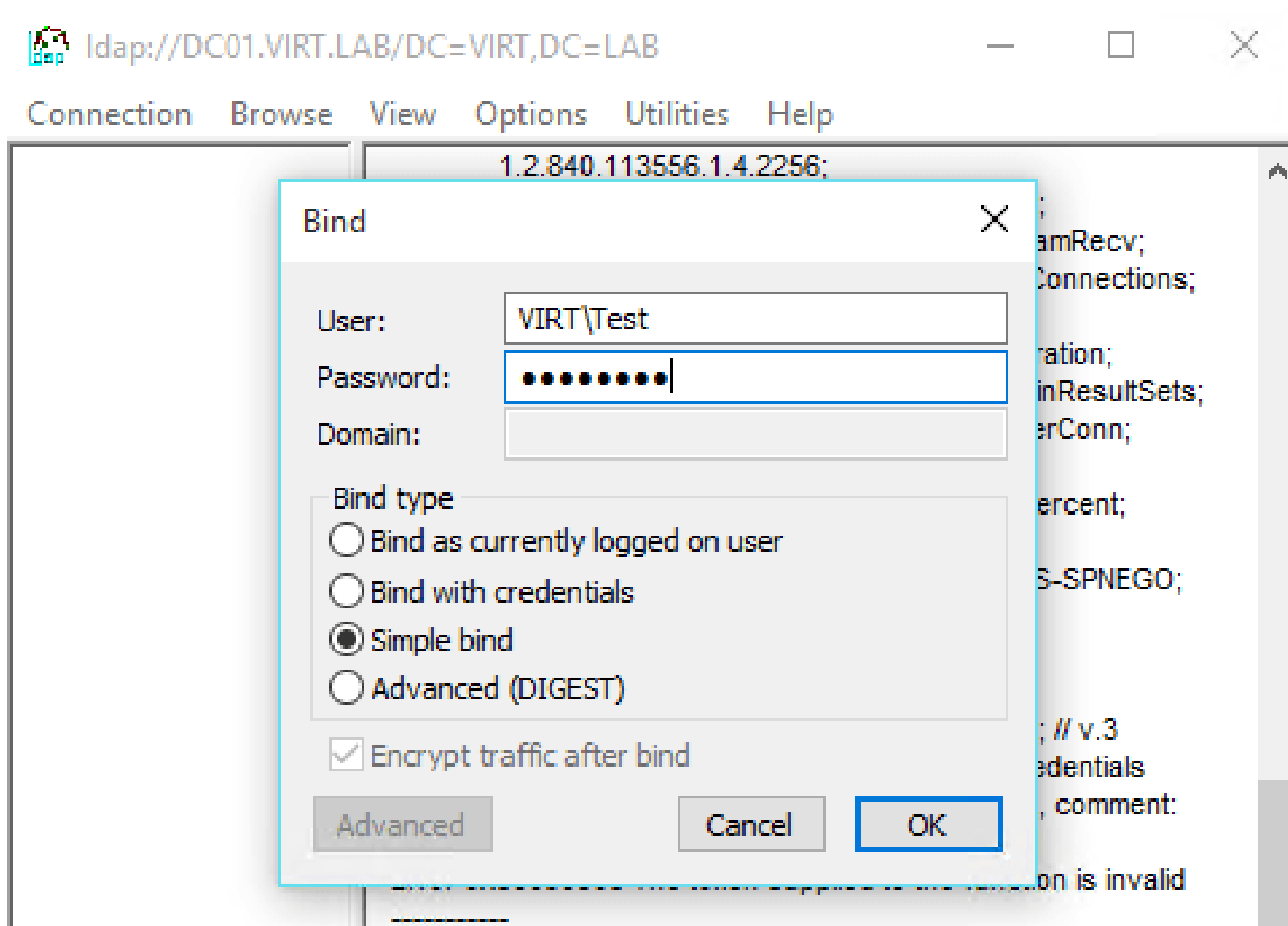
SAM-R Enumeration

Group Policy: **“Network Access: Restrict clients allowed to make remote calls to SAM”**

Registry Key: **“HKLM/System/CurrentControlSet/Control/Lsa/RestrictRemoteSAM”**

| Win version | Who can query local users by default | Can default be changed |
|----------------------------|--------------------------------------|-------------------------|
| < Win10 | Any domain user | No |
| Win10 | Any domain users | Yes (only via registry) |
| > Win10 (e.g. anniversary) | Only local administrators | Yes (registry or GPO) |

LDAP Simple Bind



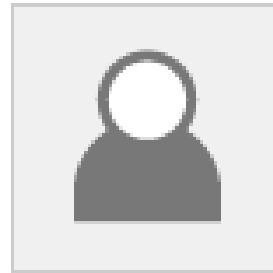
LDAP Simple Bind

Sensitive Account Credential

Test User's credentials were exp

 Note  Email  Export

 Open



Test User

VIRT.LAB

 Sensitive

 New

1 suspicious activity **1**



CHARO-Z1



DC01

Brute-Force Attack

The image shows a computer screen with three main windows:

- Web Browser:** Displays a URL `http://img812.imageshack.us/img812/2828/4f8.png[/img]` and a file named `passwords.txt`.
- DUBrute v2.1 Terminal:** A command-line interface window showing the following status:

```
DUBrute v2.1 by TeelXp
Source          0
Bad             0
Good           0
Error          0
Check          0
Thread         0
PPS            0.000
APPS           0.000
Stoped         00:00:00
```

Buttons for `Start`, `Stop`, `Config`, `Generation`, `About`, and `Exit` are visible.
- Generator IP@Login;Password GUI:** A graphical interface for configuring a brute-force attack. It has three columns: **IP**, **Login**, and **Password**. Each column has a `Clear` button, an `Add` button, and a `File` button. The `IP` list includes addresses like `82.167.173.139` and `79.188.207.18`. The `Login` list includes `Administrator`, `Administrador`, and `Administrateur`. The `Password` list includes `admin`, `enter`, `vps`, `system`, `sys`, `server`, `1234`, `123`, `13456`, `P@ssw0rd`, `Passw0rd`, and `password`.

Brute-Force Attack

Brute Force Attack Using LDAP Simple Bind

200 password guess attempts were made on 2 accounts from NINJA.

Note Email Export to Excel Details Resolved

200 guess attempts

Attacked Accounts (2)

- Administrator
- atatest

Potential Guesses (0)

None

Recommendations

- Reset the passwords of the attacked accounts
- Disconnect the relevant computers from the network or move them into an isolated environment and start a forensics procedure by investigating: unknown processes, services, registry entries, unsigned files, and more

Demo 

Encryption Downgrade

```
- reqbody:  
  + SequenceHeader:  
  + Tag0:  
  + KdcOptions: 0x40810010  
  + Tag1:  
  + Cname: administrator  
  + Tag2: 0x1  
  + Realm: contoso  
  + Tag3:  
  + Sname: krbtgt/contoso  
  + Tag5: 0x1  
  + Till: 09/13/2037 02:48:05 UTC  
  + Tag6:  
  + Rtime: 09/13/2037 02:48:05 UTC  
  + Tag7:  
  + Nonce: 1002141912 (0x3BBB78D8)  
  + Tag8:  
  - Etype:  
    + SequenceOfHeader:  
    + Etype: aes256-cts-hmac-sha1-96 (18)  
    + Etype: aes128-cts-hmac-sha1-96 (17)  
    + Etype: rc4-hmac (23)  
    + Etype: rc4-hmac-exp (24)  
    + Etype: rc4 hmac old exp (0xff79)  
    + Etype: des-cbc-md5 (3)
```

<-Etype in AS-REQ message body

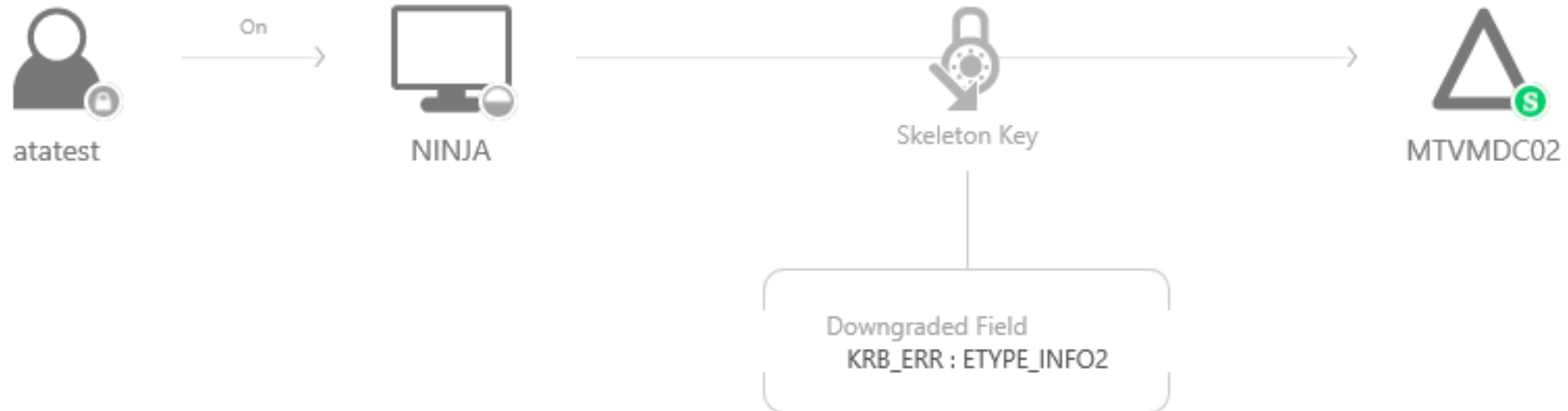
Encryption Downgrade

Encryption downgrade activity

The encryption method of the ETYPE_INFO2 field of KRB_ERR message from NINJA has been downgraded based on previously learned behavior. This may be a result of a Skeleton Key on MTVMDC02.

Note Share Export to Excel Details

Open



Recommendations

- Disconnect the relevant computers from the network or move them into an isolated environment and start a forensics procedure by investigating: unknown processes, services, registry entries, unsigned files, and more

Remote Execution Attack

Windows Sysinternals

Search TechNet with Bing



Home Learn **Downloads** Community

Windows Sysinternals > Downloads > Process Utilities > PsExec

Utilities

- [Sysinternals Suite](#)
- [Utilities Index](#)


- [File and Disk Utilities](#)
- [Networking Utilities](#)
- [Process Utilities](#)
- [Security Utilities](#)
- [System Information Utilities](#)
- [Miscellaneous Utilities](#)

Additional

PsExec v2.11

By **Mark Russinovich**

Published: May 2, 2014

 [Download PsTools](#)
(1,648 KB)

Rate: ★★★★★

Share this content     

Introduction

Utilities like Telnet and remote control programs like Symantec's PC Anywhere let you execute programs on remote systems, but they can be a pain to set up

Download



[Download PsTools](#)
(1,648 KB)

PsTools

PsExec is part of a growing kit of Sysinternals command-line tools that aid in the administration of local and remote systems named *PsTools*.

Runs on:

- Client: Windows Vista and higher.
- Server: Windows Server 2008 and higher.

Remote Execution Attack

Remote Execution Attempt Detected

There was an attempt to remotely create a service from NINJA on MTVMDC02. This may be the result of malicious activity.



Note



Email



Export to Excel



Details



Input



Dismissed

Remote execution



NINJA




MTVMDC02

Recommendations

- Disconnect NINJA from the network, or move it into an isolated environment and start a forensics procedure by investigating: unknown processes, services, registry entries, unsigned files, and more
- Investigate the root cause on NINJA
- Review MTVMDC02 for abnormal services or scheduled tasks
- Review and delete the list of suspicious files and folders on MTVMDC02


Remote Execution Attack













Remote execution attempt detected

The following remote execution attempts were performed on MTVMDC01 from NINJA:

- Successful remote creation of RemComSvc.

Thursday, June 16, 2016 at 4:29 PM  New

Summary | **Details** |  Note |  Share |  Export to Excel |  Input |  Open

| | Accounts | Created | Result | Via Domain Controllers (1) |
|--|---|---|---|--|
|  NINJA | 6/16/16 4:29 PM  Unknown |  RemComSvc %SystemRoot%\system... |  Success |  MTVMDC01 |

Demo 


Forged PAC Attack (MS14-068)

TGS-REQ


Ticket:

Ticket Granting Ticket (TGT)

Server Name: **krbtgt**
Encrypted Ticket Part (aes256-cts) [krbtgt]:

Client Name: **user**
Start: **2014-12-06 09:51:22 (UTC)**
End: **2014-12-06 19:51:22 (UTC)**
Session Key: (rc4-hmac)
e5:4f:e1:7d:8a:f6:7a:5d:76:05:e0:46:23:e3:03: 

Authenticator (rc4-hmac) [Session Key]:


Client Name: **user**
Time: **2014-12-06 09:51:22 (UTC)** 

Server Name: **krbtgt**
Encrypted Authorization Data (rc4-hmac) [Session Key]:

Privilege Attribute Certificate (PAC)

Account Name: **user**
Full Name: **Test User**
User RID: **1433**
Group Memberships:
- **513**
- **512**
- **520**
- **518**
- **519**

Server Signature (md5)
91:d1:bc:79:36:69:d6:e6:ba:ac:3b:91:c1:b8:db:89

KDC Signature (md5)
17:1a:06:4f:a5:ce:44:8b:c8:d1:47:a2:d9:13:86:a3: 

Forged PAC Attack (MS14-068)

Privilege Escalation using Forged PAC

`atatest` attempted to escalate privileges by using a forged authorization data in a Kerberos request from `NINJA` and accessing `mainstream.local` (KRBTGT) (0 successful).

 Note  Email  Export to Excel  Details

 Open



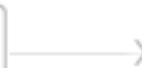
atatest

On
→



NINJA

Forged PAC



mainstream.local
to KRBTGT



MTVMDC02

Recommendations

- Disable `atatest`'s account
- Disconnect the relevant computers from the network or move them into an isolated environment and start a forensics procedure by investigating: unknown processes, services, registry entries, unsigned files, and more
- Reset the `krbtgt` domain account password twice.
- Make sure all domain controllers are up-to-date with KB3011780 (<https://support.microsoft.com/?id=3011780>).

Demo 

DCSync Attack





```
Administrator: Windows PowerShell
PS> Get-BootKey C:\ifm\registry\SYSTEM
41e34661faa0d182182f6ddf0f0ca0d1
PS> Get-ADDBAccount -DBPath 'C:\ifm\Active Directory\ntds.dit' -BootKey 41e34661faa0d182182f6ddf0f0ca0d1
>>> -DistinguishedName 'CN=krbtgt,CN=Users,DC=adatum,DC=com'

DistinguishedName: CN=krbtgt,CN=Users,DC=Adatum,DC=com
Sid: S-1-5-21-3180365339-800773672-3767752645-502
Guid: f58947a0-094b-4ae0-9c6a-a435c7d8eddb
SamAccountName: krbtgt
SamAccountType: User
UserPrincipalName:
PrimaryGroupId: 513
SidHistory:
Enabled: False
Deleted: False
LastLogon:
DisplayName:
GivenName:
Surname:
Description: Key Distribution Center Service Account
NTHash: c9467e5fae14820500862d85c53747c1
```

DCSync Attack

Malicious replication of directory services

Malicious replication requests were successfully performed from NINJA against MTVMDC02.

 Note  Share  Export to Excel  Details  Input

 Open



NINJA

Replication request



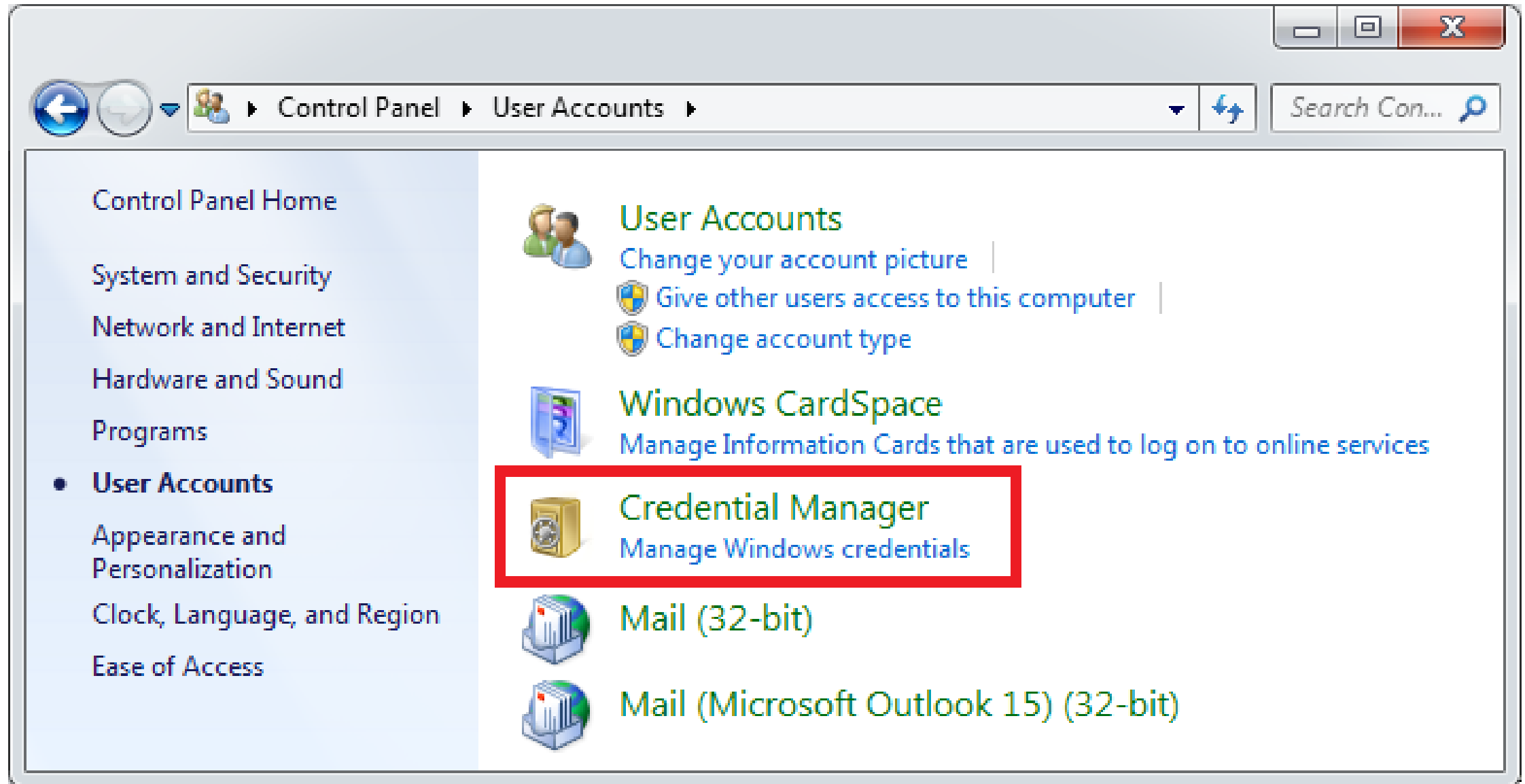
MTVMDC02

Recommendations

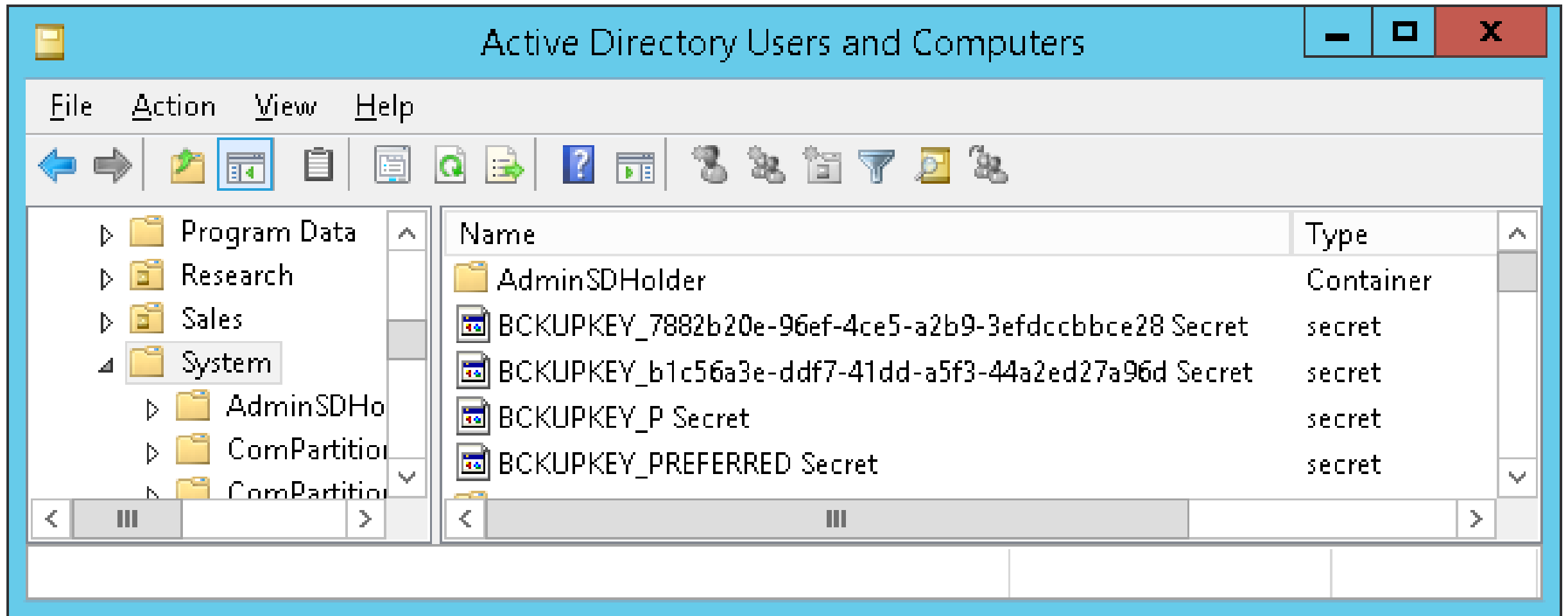
- Disconnect NINJA from the network, or move it into an isolated environment and start a forensics procedure by investigating: unknown processes, services, registry entries, unsigned files, and more
- Validate and remove permissions for users and groups who can replicate objects in Active Directory

Demo 

DPAPI Backup Key Attack



DPAPI Backup Key Attack



DPAPI Backup Key Attack

```
mimikatz # lsadump::backupkeys /export /system:lon-dc1

Current preferred key:      <b1c56a3e-ddf7-41dd-a5f3-44a2ed27a96d>
 * RSA key
   Exportable key : YES
   Key size      : 2048
   Private export : OK - 'ntds_capi_0_b1c56a3e-ddf7-41dd-a5f3-44a2ed27a96d.pvk'
   PFX container  : OK - 'ntds_capi_0_b1c56a3e-ddf7-41dd-a5f3-44a2ed27a96d.pfx'
   Export        : OK - 'ntds_capi_0_b1c56a3e-ddf7-41dd-a5f3-44a2ed27a96d.der'

Compatibility preferred key: <7882b20e-96ef-4ce5-a2b9-3efdccbbce28>
 * Legacy key
4d8afa06d73f999fd8467d7de30b5f67a3b9d7ff143360246a96a14c8a11d732
b5c6707262a4108c150e964aaa164871e15610ab66123283bb083a1fea9b3718
699bbb0d6e9463ecd8302ddb3f3b6911dd7e624d80e469b4cd88dc555f16d59e
48fb6daa5603f150bb449f843c647f7a4373442791d8d215e9fad8265741dec5
c7bce4e530be180ee6f645a42f30925554d8610cab903b3390705bbad4193251
0d8fc2fdc992cc38c133ec1fb61de2c45b4e59abd753bf28ec538d4de1ff0e37
29fe55b6f07633d8d1e3b99762dbf172cfa10801a0eb51b54b86766c184f60a1
d73941e292fe842b403a06affcc825be90a49c4adafbccef0c674bf81cd37ad9

Export      : OK - 'ntds_legacy_0_7882b20e-96ef-4ce5-a2b9-3efdccbbce28.key'
```

DPAPI Backup Key Attack

Malicious Data Protection Private Information Request

An unknown user performed 4 successful attempts from MTVMATA01 to retrieve DPAPI domain backup key from 2 domain controllers.

Note Share Export to Excel Details

Open



Recommendations

- Disconnect MTVMATA01 from the network, or move it into an isolated environment and start a forensics procedure by investigating: unknown processes, services, registry entries, unsigned files, and more
- Disable the relevant accounts

Demo 

Pass-the-Ticket Attack

```
C:\Windows\system32\cmd.exe
C:\Users\test.user>klist

Current LogonId is 0:0x23111

Cached Tickets: (5)

#0>      Client: test.user @ LAB.LOCAL
        Server: krbtgt/LAB.LOCAL @ LAB.LOCAL
        KerbTicket Encryption Type: RSADSI RC4-HMAC<NT>
        Ticket Flags 0x60a00000 -> forwardable forwarded renewable pre_authent
        Start Time: 2/16/2015 8:51:59 <local>
        End Time: 2/16/2015 18:51:54 <local>
        Renew Time: 2/23/2015 8:51:54 <local>
        Session Key Type: RSADSI RC4-HMAC<NT>

#1>      Client: test.user @ LAB.LOCAL
        Server: krbtgt/LAB.LOCAL @ LAB.LOCAL
        KerbTicket Encryption Type: RSADSI RC4-HMAC<NT>
        Ticket Flags 0x40e00000 -> forwardable renewable initial pre_authent
        Start Time: 2/16/2015 8:51:54 <local>
        End Time: 2/16/2015 18:51:54 <local>
        Renew Time: 2/23/2015 8:51:54 <local>
        Session Key Type: RSADSI RC4-HMAC<NT>

#2>      Client: test.user @ LAB.LOCAL
        Server: cifs/win2k8-dc.lab.local @ LAB.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40a40000 -> forwardable renewable pre_authent ok_as_delegate
        Start Time: 2/16/2015 8:51:59 <local>
        End Time: 2/16/2015 18:51:54 <local>
        Renew Time: 2/23/2015 8:51:54 <local>
        Session Key Type: AES-256-CTS-HMAC-SHA1-96

#3>      Client: test.user @ LAB.LOCAL
        Server: ldap/win2k8-dc.lab.local @ LAB.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40a40000 -> forwardable renewable pre_authent ok_as_delegate
        Start Time: 2/16/2015 8:51:59 <local>
        End Time: 2/16/2015 18:51:54 <local>
        Renew Time: 2/23/2015 8:51:54 <local>
```

Pass-the-Ticket Attack

Identity Theft Using Pass-the-Ticket Attack

Grafnetter Michael's Kerberos tickets were stolen from MAIN024NB to NINJA and used to access 3 resources.

Note Email Export to Excel Details Input Resolved



Recommendations

- Disconnect the relevant computers from the network or move them to a secure location for investigation: unknown processes, services, registry entries, unsolicited connections, etc.
- Disable Grafnetter Michael's account

Resources (3)

- MTVMDC02 to CIFS
- MAINSTREAM.LOCAL to KRBTGT
- MTVMDC03 to CIFS

Procedure by

Demo 

Pass-the-Hash Attack

```
mimikatz 2.0 alpha x64 (oe.eo)
mimikatz # sekurlsa::pth /user:Administrator /domain:adatum.com /ntlm:8c2f03f739967680445fb6433fec5ca4 /
5d9cf30af8f6cf8530d1e20e8 /run:mmc
user      : Administrator
domain    : adatum.com
program   : mmc
AES256    : 392ae7a4f2ef064117552b1c155ee494116b7c85d9cf30af8f6cf8530d1e20e8
NTLM      : 8c2f03f739967680445fb6433fec5ca4
| PID 3548
| TID 2736
| LUID 0 ; 2601234 (00000000:0027b112)
\_ msv1_0 - data copy @ 0000006CB84955E0 : OK !
\_ kerberos - data copy @ 0000006CB84C0248
  \_ aes256_hmac      OK
  \_ aes128_hmac     -> null
  \_ rc4_hmac_nt     OK
  \_ rc4_hmac_old    OK
  \_ rc4_md4         OK
  \_ rc4_hmac_nt_exp OK
  \_ rc4_hmac_old_exp OK
  \_ *Password replace -> null
```

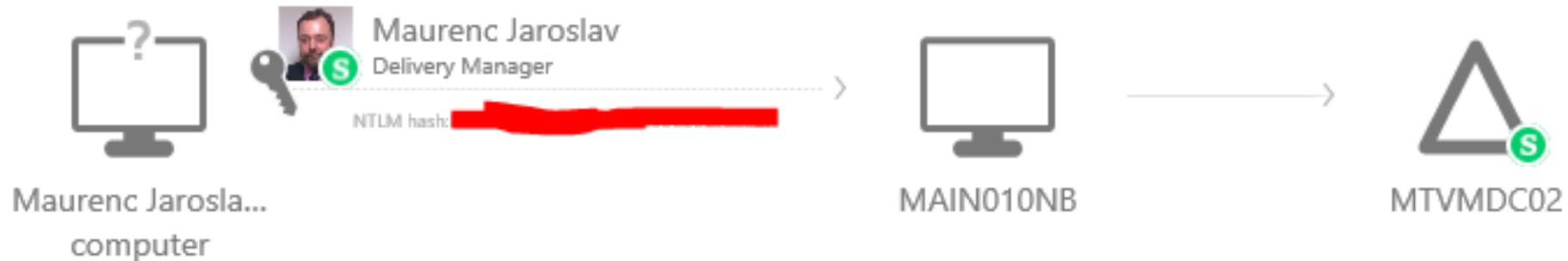
Pass-the-Hash Attack

Identity Theft Using Pass-the-Hash Attack

Maurenc Jaroslav's hash was stolen from one of the computers previously logged into by Maurenc Jaroslav and used from MAIN010NB.

 Note  Email  Export to Excel

 Resolved



Recommendations

- Disconnect the relevant computers from the network or move them into an isolated environment and start a forensics procedure by investigating: unknown processes, services, registry entries, unsigned files, and more
- Disable Maurenc Jaroslav's account
- Reset Maurenc Jaroslav's password

Suspicious Activity

Suspicion of Identity Theft Based on Abnormal Authentication or Resource Access Behavior

Michael Dubinsky exhibited abnormal behavior based on the following activities:

- Performed interactive login from 6 abnormal workstations.
- Performed interactive login from SharedAdmin-SRV.
- Requested access to 6 abnormal resources.

 Note  Email  Export to Excel  Details

 Open



Michael Dubinsky
SR PROGRAM MANAGER



2 Normal
computers



7 Abnormal
computers

Accessed



2 Normal
resources































6 Abnormal
resources


Recommendations

- Disconnect the relevant computers from the network or move them into an isolated environment and start a forensics procedure by investigating: unknown processes, services, registry entries, unsigned files, and more
- Contact Michael Dubinsky and investigate if the user has logged in to abnormal computers and accessed abnormal resources.

Suspicious Activity

|  Michael Dubinsky SR PROGRAM MANAG... | | From (9) | Accessed (8) | Via Domain Controllers (1) |
|--|--|---|--|--|
| 10:47 PM Wednesday March 25, 2015 |  Michael-Desk 10.20.20.11 | |  DC to KRBTGT |  DC 10.20.30.1 |
| 10:47 PM Thursday March 26, 2015 |  Michael's-iPad 10.20.20.214 | |  DC to KRBTGT |  DC 10.20.30.1 |
| 11:37 PM Wednesday April 15, 2015 |  ExtVendor-PC 10.20.30.101 |  |  AORATO.COM to KRBTGT |  DC 10.20.30.1 |
| 11:59 PM Wednesday April 15, 2015 |  SharedAdmin-SRV 10.20.30.40 |  |  SharedAdmin-SRV to CIFS |  DC 10.20.30.1 |
| 11:59 PM Wednesday April 15, 2015 |  SharedAdmin-SRV 10.20.30.40 |  |  DC to KRBTGT |  DC 10.20.30.1 |
| 11:59 PM Wednesday April 15, 2015 |  Test-PC 10.44.50.15 | |  HRWeb to HTTP |  DC 10.20.30.1 |
| 11:59 PM Wednesday April 15, 2015 |  Test-PC 10.44.50.15 | |  DC to KRBTGT |  DC 10.20.30.1 |
| 11:59 PM |  InComm-PC | |  FINANCE DOCS |  DC |

Honeytoken



Administrator

Built-in account for administering the computer/domain

mainstream.local
Created on Jun 18, 2006
Administrator@mainstream.cz

S Sensitive ⏸ Disabled 🔒 Locked

2 suspicious activities 2 Medium


- Summary
- Activities
- Suspicious activities

Memberships (4)

- S Domain Admins
Designated administrators of the dom...
- S Group Policy Creator Own...
Members in this group can modify gro...
- Domain Users
All domain users
- S Administrators
Administrators have complete and unr...

User activity

■ NTLM ■ LDAP Bind ■ Kerberos



| Activity Type | Start Value | End Value |
|---------------|-------------|-----------|
| NTLM | 30 | 50 |
| LDAP Bind | 60 | 50 |
| Kerberos | 30 | 50 |

Honeytoken

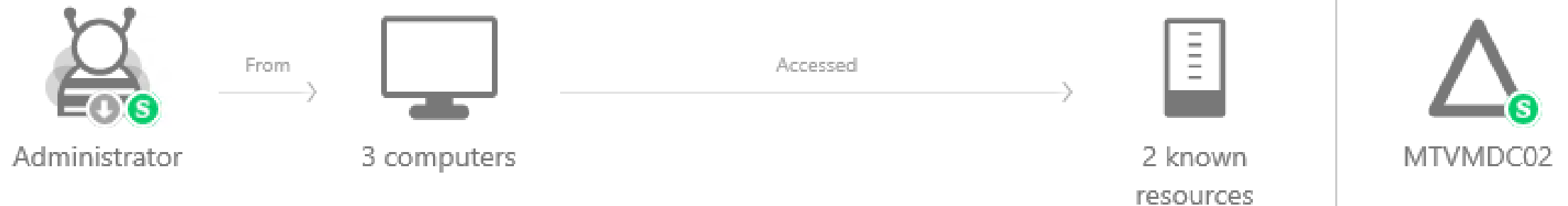
Honeytoken activity

The following activities were performed by Administrator:

- Attempted to authenticate from NINJA using LDAP simple bind when accessing MTVMDC02 (LDAP) on MTVMDC02.
- Attempted to authenticate from 3 computers using NTLM when accessing MTVMDC02 (LDAP) on MTVMDC02.

 Note  Share  Export to Excel  Details

 Open



Recommendations

- Disconnect the relevant computers from the network or move them into an isolated environment and start a forensics procedure by investigating: unknown processes, services, registry entries, unsigned files, and more

Demo 

Broken Trust



The trust relationship between this workstation and the primary domain failed.

OK



Windows Server 2008
Enterprise

Broken Trust

Computers' Broken Trust Relationship

The trust relationship between MTVMDA and the domain is broken.

- Group policy is not applied (security violation)
- Users cannot log into the computers.

 Note  Email  Export to Excel

 Resolved



MTVMDC02

Recommendations

- Rejoin or remove the computers from the domain



Microsoft ATA Licensing Options



Microsoft ATA Licensing

| | Per user | Per OSE*/device |
|---|----------|-----------------|
| Through Enterprise CAL Suite per-user license | ● | |
| Through Enterprise CAL Suite per-device license | | ● |
| Through Enterprise Mobility Suite user subscription license | ● | |
| Through Enterprise Cloud Suite user subscription license | ● | |
| Standalone license - Open L&SA estimated retail price, annualized** | USD \$80 | USD \$61.50 |

Enterprise CAL Suite

Windows Server
Active Directory
Rights Management
Services CAL

Exchange Server
Enterprise CAL with
Services

SharePoint Server
Enterprise CAL

Skype for Business
Server Enterprise CAL

Exchange Online
Archiving for
Exchange Server

Advanced Threat
Analytics

Windows Server CAL

Exchange Server
Standard CAL

SharePoint Server
Standard CAL

Skype for Business
Server Standard CAL

System Center
Configuration
Manager CML

System Center
Endpoint Protection

Core CAL Suite

Enterprise Mobility Suite

- Advanced Threat Analytics
- Azure AD Premium (incl. Multi-Factor Authentication)
- Microsoft Intune
- Azure RMS
- Azure RemoteApp
- Microsoft Identity Manager



Enterprise Cloud Suite

Office 365

Office 365 Pro Plus
Exchange Online
Lync Online
SharePoint Online
Yammer

EMS

System Center CM
Windows Server CAL
Azure Rights Management
Windows Intune
Azure AD Premium

Windows SA Per User

Twitter



| TWEETS | FOLLOWING | FOLLOWERS | LIKES | LISTS |
|--------|-----------|-----------|-------|-------|
| 222 | 52 | 500 | 38 | 1 |

Idan Plotnik
@IdanPlotnik

Surfer, Tech and Business Geek,
Founder and CEO @Aorato, Now
Director Group Manager @Microsoft
Security Division

New York

[Tweet to Idan Plotnik](#)

4 Followers you know



[Photos and videos](#)

Tweets Tweets & replies Media

Idan Plotnik Retweeted

 **Michael Grafnetter** @MGrafnetter · 9m
[@gentilkiwi](#) [@IdanPlotnik](#) [@TalBeerySec](#) [@MichaelDubinsky](#) Love this new release. Bet that Hacking Team wish they had [#MicrosoftATA](#) in place ;-)

[View conversation](#)

 **Idan Plotnik** @IdanPlotnik · 14m
You want to know why [#MicrosoftATA](#) is the pioneer and leader in the [@Gartner_inc](#) [#UEBA](#) market? pen-test and compare against competitors

Twitter



Tal Be'ery
@TalBeerySec FOLLOWS YOU

Security Research Manager. VP of Research @Aorato acquired by @Microsoft. Building #MicrosoftATA.

Israel
[linkedin.com/in/talbeery](https://www.linkedin.com/in/talbeery)
Joined April 2014

[Tweet to](#) [Message](#)

10 Followers you know

Tweets Tweets & replies Media

Tal Be'ery @TalBeerySec · 22 Feb 2015

OMG! i'm in RFC!
tools.ietf.org/html/rfc7457#r...

[TIME] Be'ery, T. and A. Shulman "A Perfect CRIME? Only TIME will tell", Black Hat Europe 2013, 2013, <<https://media.blackhat.com/eu-13/briefings/Beery/bh-eu-13-a-perfect-crime-beery-wp.pdf>>.

Sheffer, et al. Informational [Page 12]

DEC 7457 TIC Attacks February 2015



Microsoft Advanced Threat Analytics

Mgr. Michael Grafnetter

Architect

