Microsoft Advanced Threat Analytics

Mgr. Michael Grafnetter
Architect

mainstream TECHNOLOGIES
Agenda

- ATA Overview
- ATA Deployment and Configuration
- Live Hacking Session
Advanced Infrastructure Attacks
Lateral Movement

GET CREDENTIALS
Malicious tactics such as social engineering and phishing schemes are used to trick personnel and obtain credentials for network access. Most organizations do not recognize when attackers are already within the network and have access to information such as emails, confidential documents, and other intellectual property.

GET DATA
The attack doesn’t stop there. Attackers look for the next set of credentials with elevated permissions to access servers. Once elevated credentials are obtained, servers are compromised, organization risk losing revenue, brand reputation, and business continuity.

GET CONTROL
The ultimate goal of the attackers may be to gain access to the domain controllers, the central clearing hub for all credentials and identities. Once compromised, an attacker has complete control over an entire organization. All assets, intellectual property, physical property, and personal information are at jeopardy.

ELAPSED TIME: 0 HRS OR LESS

ELAPSED TIME: 24 HRS OR LESS

ELAPSED TIME: 48 HRS OR LESS
Advanced Hacking Tools

```
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>
```
Motivated Hackers
Common Cyber Attacks: Reducing The Impact

Most cyber attacks are composed of four stages: Reconnaissance, Delivery, Breach, and Impact. 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

Who might be attacking you?
Cyber criminals are interested in making money through fraud or the sale of valuable information. Industrial competitors and foreign intelligence services interested in gaining an economic advantage for their companies or countries.
Hackers who find interfering with computer systems an enjoyable challenge.
Honeypots who wish to attack companies for political or ideological motives.
Employees, or those who have legitimate access, denied by accidents or deliberate misuse.

Survey
Websites
Controls For The Attack Stage
User Education
Training all users on what they should avoid in published resources and web content.

Network Perimeter Defences
Can block suspicious or malicious traffic services, or only allow trusted websites to be accessed.

Password Policy
Can prevent users from selecting simple passwords and lockout accounts after too many unsuccessful attempts.

Device Controls
Deny the access to the internal gateway should be used to prevent unauthorised access to critical servers and services that may still be required.

Secure Configuration
Remove unnecessary software and default user accounts. Ensure default passwords are changed, and that automatic updates are turned off.

User Access
Well-maintained user access controls can restrict access to the applications, printers, and data that users can access.

User Training
User training is extremely valuable in reducing the likelihood of successful social engineering attacks.

Malware Protection
Malware protection within the internet gateway can detect malicious code in an infected form.

Privacy Management
Privacy policies and procedures to identify any malicious or unusual activity.

Monitoring
Monitor and analyse all network activity to identify any malicious or unusual activity.

Patch Management
Apply patches at the correct time to limit exposure to known software vulnerabilities.

Device Configuration
When necessary, install or remove software on the device.

Device Controls
Deny the access to the internal gateway should be used to prevent unauthorised access to critical servers and services that may still be required.
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.
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.
Introducing Microsoft Advanced Threat Analytics

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

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
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.
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

---

**Reconnaissance**
- 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

**Compromised Credential**

**Lateral Movement**

**Privilege Escalation**
- MS14-068 exploit (Forged PAC)
- MS11-013 exploit (Silver PAC)

**Domain Domination**
What ATA Detects

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

Iran hacked an American casino

"FIN6" Cybergang Steals Millions of Cards From PoS Systems

How Hacking Team got hacked

A black hat claims responsibility for the hack. Here's how he says he did it.
63% of confirmed data breaches involved weak, default or stolen passwords.
ATA Architecture

Port Mirroring (Network DPI)

Windows Event Forwarding (WEF)

Syslog Forwarding

ATA Gateway

ATA Center

SIEM
Fileserever
DB

DC4
DC3

DC2
DC1

ATA Lightweight Gateway
ATA Lightweight Gateway

ATA Lightweight Gateway
ATA Lightweight Gateway
<table>
<thead>
<tr>
<th>Time (UTC)</th>
<th>Source Ip Address</th>
<th>Source Port</th>
<th>Destination Ip Address</th>
<th>Destination Port</th>
<th>Transport Protocol</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>5/12/2016 1:00:48 AM</td>
<td>192.168.110.11</td>
<td>43392</td>
<td>172.27.126.10</td>
<td>88</td>
<td>Top</td>
<td>KerberosAs</td>
</tr>
<tr>
<td>5/12/2016 1:09:52 AM</td>
<td>192.168.110.11</td>
<td>43418</td>
<td>172.27.126.10</td>
<td>88</td>
<td>Top</td>
<td>KerberosAs</td>
</tr>
<tr>
<td>5/12/2016 1:09:53 AM</td>
<td>192.168.110.11</td>
<td>43419</td>
<td>172.27.126.10</td>
<td>88</td>
<td>Top</td>
<td>KerberosAs</td>
</tr>
<tr>
<td>5/12/2016 1:12:752 AM</td>
<td>192.168.110.11</td>
<td>43423</td>
<td>172.27.126.10</td>
<td>88</td>
<td>Top</td>
<td>KerberosAs</td>
</tr>
<tr>
<td>5/12/2016 1:12:75 AM</td>
<td>192.168.110.11</td>
<td>43429</td>
<td>172.27.126.10</td>
<td>88</td>
<td>Top</td>
<td>KerberosAs</td>
</tr>
<tr>
<td>5/12/2016 1:13:003 AM</td>
<td>192.168.110.11</td>
<td>43431</td>
<td>172.27.126.10</td>
<td>88</td>
<td>Top</td>
<td>KerberosAs</td>
</tr>
<tr>
<td>5/12/2016 1:13:013 AM</td>
<td>192.168.110.11</td>
<td>43432</td>
<td>172.27.126.10</td>
<td>88</td>
<td>Top</td>
<td>KerberosAs</td>
</tr>
<tr>
<td>5/12/2016 1:16:514 AM</td>
<td>192.168.110.11</td>
<td>43e32</td>
<td>172.27.126.10</td>
<td>88</td>
<td>Top</td>
<td>KerberosAs</td>
</tr>
</tbody>
</table>
ATA Deployment and Configuration
ATA Center RBAC
Configuration – ATA Gateway – Hyper-V

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

Router guard
Router guard drops router advertisement and redirection messages from unauthorized virtual machines pretending to be routers.

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
## Configuration - Detection

<table>
<thead>
<tr>
<th></th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Short-term lease subnets</td>
<td>157.54.208.0/24 or 3FFE:FFFF:0:0000::/64</td>
</tr>
<tr>
<td></td>
<td>92.168.0.0/24</td>
</tr>
<tr>
<td>Honeytoken account SIDs</td>
<td>S-1-5-21-72081277-1610778489-2625714895-10511</td>
</tr>
<tr>
<td>DNS Reconnaissance IP address exclusions</td>
<td></td>
</tr>
<tr>
<td>Pass-the-Ticket IP address exclusions</td>
<td></td>
</tr>
</tbody>
</table>

[Save]
Identity Theft Using Pass-the-Ticket Attack
MAIN019NB's Kerberos tickets were stolen from MTVMDA to MAIN019NB and used to access 2 resources.

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

Computers (2)

- MAIN019NB
  - Yes

- MTVMDA
  - Yes
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**

<table>
<thead>
<tr>
<th>MTVMEX03</th>
<th>Accessed</th>
</tr>
</thead>
<tbody>
<tr>
<td>MTVMEX03</td>
<td></td>
</tr>
</tbody>
</table>

**Input**

- Resolved
- Dismissed

31 normal resources + 3 abnormal resources
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.
MongoDB
Integration - SIEM

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

Syslog server endpoint: nagios.mainstream.local : 514

Transport: UDP

Format: RFC 5424

RFC 3164
Integration - SCOM

The Event Viewer window is displayed, showing Microsoft ATA events. The table contains the following entries:

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

Event 0, Microsoft ATA

General | Details

Bubnik Karel's hash was stolen from one of the computers previously logged into by Bubnik Karel and used from MAIN054NB.
Integration – Azure OMS

NOTABLE ISSUES

Active issue types

<table>
<thead>
<tr>
<th>Name</th>
<th>Count</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft ATA: suspicious user behavior</td>
<td>3K</td>
<td>!</td>
</tr>
<tr>
<td>Microsoft ATA: health error</td>
<td>300</td>
<td>!</td>
</tr>
<tr>
<td>Detections of suspicious process exec...</td>
<td>6</td>
<td>!</td>
</tr>
<tr>
<td>Computers with cleaned event logs</td>
<td>1</td>
<td>!</td>
</tr>
<tr>
<td>Computers with system audit policy ch...</td>
<td>1</td>
<td>!</td>
</tr>
<tr>
<td>Microsoft ATA: suspicious user behavior</td>
<td>600</td>
<td>!</td>
</tr>
</tbody>
</table>
## Integration – Azure OMS

### Microsoft Operations Management Suite

#### Search

**Data based on last 7 days**

**1 bar = 6 hrs**

**TYPE (1)** Security\n
**COMPUTER (1)** OrcoOMSProdPub

**ALERTSEVERITY (2)** high

**ALERTTITLE (2)** Suspicious Activity

<table>
<thead>
<tr>
<th>TimeGenerated</th>
<th>Computer</th>
<th>AlertSeverity</th>
<th>Description</th>
<th>AlertTitle</th>
<th>SourceSystem</th>
<th>Provider</th>
<th>OriginalSeverity</th>
</tr>
</thead>
<tbody>
<tr>
<td>5/25/2016 10:43:58 AM</td>
<td>OrcoOMSProdPub</td>
<td>High</td>
<td>Administrator successfully authenticated from CLIENT23 against DCT using an unusual protocol implementation. This may</td>
<td>Suspicious Activity</td>
<td></td>
<td>Microsoft ATA</td>
<td>2</td>
</tr>
<tr>
<td>5/25/2016 10:43:58 AM</td>
<td>OrcoOMSProdPub</td>
<td>High</td>
<td>SMB session enumeration attempts failed from CLIENT23 against DCT. No accounts were exposed.</td>
<td>Suspicious Activity</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Additional Information

- **TimeGenerated**: 5/25/2016 10:43:58 AM
- **Computer**: OrcoOMSProdPub
- **AlertSeverity**: High
- **Description**: Administrator successfully authenticated from CLIENT23 against DCT using an unusual protocol implementation. This may
- **AlertTitle**: Suspicious Activity
- **SourceSystem**: OMS
- **Provider**: Microsoft ATA
- **OriginalSeverity**: 2

### Show Less

- **TimeGenerated**: 5/25/2016 10:43:58 AM
- **Computer**: OrcoOMSProdPub
- **AlertSeverity**: High
- **Description**: SMB session enumeration attempts failed from CLIENT23 against DCT. No accounts were exposed.
- **AlertTitle**: Suspicious Activity

### Show More

- **TimeGenerated**: 5/25/2016 10:43:58 AM
- **Computer**: OrcoOMSProdPub
- **AlertSeverity**: Low
- **Description**: The following remote execution attempts were performed on DCT from CLIENT1: Successful remote creation of Fog\n- **AlertTitle**: Suspicious Activity

### Show More
Microsoft Advanced Threat Analytics

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

<table>
<thead>
<tr>
<th>PACKETS PER SECOND*</th>
<th>CPU (CORES**)</th>
<th>MEMORY (GB)</th>
<th>DATABASE STORAGE PER DAY (GB)</th>
<th>DATABASE STORAGE PER MONTH (GB)</th>
<th>IOPS***</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,000</td>
<td>2</td>
<td>32</td>
<td>0.3</td>
<td>9</td>
<td>30 (100)</td>
</tr>
<tr>
<td>10,000</td>
<td>4</td>
<td>48</td>
<td>3</td>
<td>90</td>
<td>200 (300)</td>
</tr>
<tr>
<td>40,000</td>
<td>8</td>
<td>64</td>
<td>12</td>
<td>360</td>
<td>500 (1,000)</td>
</tr>
<tr>
<td>100,000</td>
<td>12</td>
<td>96</td>
<td>30</td>
<td>900</td>
<td>1,000 (1,500)</td>
</tr>
<tr>
<td>400,000</td>
<td>40</td>
<td>128</td>
<td>120</td>
<td>1,800</td>
<td>2,000 (2,500)</td>
</tr>
</tbody>
</table>
## Capacity Planning - ATA Lightweight GW

<table>
<thead>
<tr>
<th>Packets Per Second*</th>
<th>CPU (Cores**)</th>
<th>Memory (GB)**</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,000</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>5,000</td>
<td>6</td>
<td>16</td>
</tr>
<tr>
<td>10,000</td>
<td>10</td>
<td>24</td>
</tr>
</tbody>
</table>
## Capacity Planning – ATA Gateway

<table>
<thead>
<tr>
<th>Packets Per Second*</th>
<th>CPU (Cores**)</th>
<th>Memory (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,000</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>5,000</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>10,000</td>
<td>3</td>
<td>12</td>
</tr>
<tr>
<td>20,000</td>
<td>6</td>
<td>24</td>
</tr>
<tr>
<td>50,000</td>
<td>16</td>
<td>48</td>
</tr>
</tbody>
</table>
Dropped port mirrored network traffic
ATA Gateway, CZES0001ATAG001, 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
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
## Monitoring ATA Performance

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft ATA Center AppDomainManager UpdateExceptionStatistics Time</td>
<td>0.00</td>
</tr>
<tr>
<td>CenterConfigurationManager UpdateConfiguration Time</td>
<td>66.00</td>
</tr>
<tr>
<td>CenterDatabaseClient BackupSystemProfiles Time</td>
<td>28.00</td>
</tr>
<tr>
<td>CenterDatabaseClient DeleteOldCollections Time</td>
<td>28.00</td>
</tr>
<tr>
<td>CenterDatabaseClient DirectoryServicesActivities Block Input Items/Sec</td>
<td>0.00</td>
</tr>
<tr>
<td>CenterDatabaseClient DirectoryServicesActivities Block Output Batch Size</td>
<td>1.00</td>
</tr>
<tr>
<td>CenterDatabaseClient DirectoryServicesActivities Block Output Items/Sec</td>
<td>0.00</td>
</tr>
<tr>
<td>CenterDatabaseClient DirectoryServicesActivities Block Size</td>
<td>0.00</td>
</tr>
<tr>
<td>CenterDatabaseClient DirectoryServicesActivities Block Time</td>
<td>2.00</td>
</tr>
<tr>
<td>CenterDatabaseClient Dnss Block Input Items/Sec</td>
<td>0.00</td>
</tr>
<tr>
<td>CenterDatabaseClient Dnss Block Output Batch Size</td>
<td>1.00</td>
</tr>
<tr>
<td>CenterDatabaseClient Dnss Block Output Items/Sec</td>
<td>0.00</td>
</tr>
<tr>
<td>CenterDatabaseClient Dnss Block Size</td>
<td>0.00</td>
</tr>
<tr>
<td>CenterDatabaseClient Dnss Block Time</td>
<td>39.00</td>
</tr>
<tr>
<td>CenterDatabaseClient KerberosAps Block Input Items/Sec</td>
<td>0.00</td>
</tr>
<tr>
<td>CenterDatabaseClient KerberosAps Block Output Batch Size</td>
<td>1.00</td>
</tr>
</tbody>
</table>
Live Hacking Session
DNS Reconnaissance

Command Prompt - nslookup - 192.168.110.31

> ls mainstream.cz
[mtvmdc02.mainstream.local]
mainstream.cz. NS service01.mainstream.local
mainstream.cz. NS service02.mainstream.local
mainstream.cz. NS service03.mainstream.local
mainstream.cz. NS service02.mainstream.local
admin A 192.168.110.31
autodiscover A 192.168.110.31
cloud A 192.168.110.31
tx A 192.168.110.31
da A 192.168.110.31
directaccess A 193.168.110.31
fs A 10.6.0.2
helpdesk A 192.168.110.31
im A 172.168.110.31
intranet A 172.168.110.31
jira A 192.168.110.31
DNS Reconnaissance

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

Exposed Accounts (4)

- SECRETS-DB\$ on 192.168.0.210
- user1 on 192.168.0.1
- APP2\$ 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.
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
SAM-R Enumeration

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

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

<table>
<thead>
<tr>
<th>Win version</th>
<th>Who can query local users by default</th>
<th>Can default be changed</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; Win10</td>
<td>Any domain user</td>
<td>No</td>
</tr>
<tr>
<td>Win10</td>
<td>Any domain users</td>
<td>Yes (only via registry)</td>
</tr>
<tr>
<td>&gt; Win10 (e.g. anniversary)</td>
<td>Only local administrators</td>
<td>Yes (registry or GPO)</td>
</tr>
</tbody>
</table>
LDAP Simple Bind

User: VIRT\Test
Password: ********
Domain: 

Bind type
- Bind as currently logged on user
- Bind with credentials
- Simple bind
- Advanced (DIGEST)

Encrypt traffic after bind

Advanced
Cancel
OK
LDAP Simple Bind

Sensitive Account Credential
Test User's credentials were exposed

Test User
VIRT.LAB

1 suspicious activity

CHARO-Z1

DC01
Brute-Force Attack
Brute-Force Attack

Brute Force Attack Using LDAP Simple Bind
200 password guess attempts were made on 2 accounts from NINJA.

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

- Keybody:
  + SequenceHeader:
  + Tag0:
  + KdcOptions: 0x40810010
  + Tag1:
  + Cname: administrator
  + Tag2: 0x1
  + Realm: contoso
  + Tag3:
  + Sname: krbtgt/contoso
  + Tag5: 0x1
  + Ti1l: 09/13/2037 02:48:05 UTC
  + Tag6:
  + Rtime: 09/13/2037 02:48:05 UTC
  + Tag7:
  + Nonce: 1002141912 (0x3BBB78D8)
  + Tag8:
    + 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)
Encryption Downgrade

Encryption downgrade activity

The encryption method of the ETYP_INFO2 field of KRBB_ERR message from NINJA has been downgraded based on previously learned behavior. This may be a result of a Skeleton Key on MTVMDC02.

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

Utilities

- Sysinternals Suite
- Utilities Index
- File and Disk Utilities
- Networking Utilities
- Process Utilities
- Security Utilities
- System Information Utilities
- Miscellaneous Utilities

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.
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.

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

<table>
<thead>
<tr>
<th>Accounts</th>
<th>Created</th>
<th>Result</th>
<th>Via Domain Controllers (1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown</td>
<td>RemComSvc %SystemRoot\system32\svchost.exe</td>
<td>✔ Success</td>
<td>MTVMDC01</td>
</tr>
</tbody>
</table>
Demo
Forged PAC Attack (MS14-068)
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).

--

<table>
<thead>
<tr>
<th>Note</th>
<th>Email</th>
<th>Export to Excel</th>
<th>Details</th>
<th>Open</th>
</tr>
</thead>
</table>

![Diagram]

Forged PAC

<table>
<thead>
<tr>
<th>atatest</th>
<th>NINJA</th>
<th>mainstream.local to KRBTGT</th>
<th>MTVMDC02</th>
</tr>
</thead>
</table>

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

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

DistinguishedName: CN=krbtg,CN=Users,DC=Adatum,DC=com
Sid: S-1-5-21-3180365339-800773672-3767752645-502
Guid: f58947a0-094b-4ae0-9c6a-a435c7d83edbb
SamAccountName: krbtgt
SamAccountType: User
PrimaryPrincipalName:
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.

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

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

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

```
\textbf{Client: test.user @ LAB.LOCAL}
\textbf{Server: krbtgt/LAB.LOCAL @ LAB.LOCAL}
\textbf{KerbTicket Encryption Type: RSADSI RC4-HMAC(N}}
\textbf{Ticket Flags 0x00000000 -> forwardable forwarded renewable pre_authent}
\textbf{Start Time: 2/16/2015 8:51:59 <local>}
\textbf{End Time: 2/16/2015 18:51:58 <local>}
\textbf{Renew Time: 2/23/2015 8:51:54 <local>}
\textbf{Session Key Type: RSADSI RC4-HMAC(N}}

\textbf{Client: test.user @ LAB.LOCAL}
\textbf{Server: krbtgt/LAB.LOCAL @ LAB.LOCAL}
\textbf{KerbTicket Encryption Type: RSADSI RC4-HMAC(N}}
\textbf{Ticket Flags 0x00000000 -> forwardable renewable initial pre_authent}
\textbf{Start Time: 2/16/2015 8:51:59 <local>}
\textbf{End Time: 2/16/2015 18:51:54 <local>}
\textbf{Renew Time: 2/23/2015 8:51:54 <local>}
\textbf{Session Key Type: RSADSI RC4-HMAC(N}}

\textbf{Client: test.user @ LAB.LOCAL}
\textbf{Server: cifc/win2k8-de.lab.local @ LAB.LOCAL}
\textbf{KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96}
\textbf{Ticket Flags 0x00000000 -> forwardable renewable pre_authent ok_as_delegate}
\textbf{Start Time: 2/16/2015 8:51:59 <local>}
\textbf{End Time: 2/16/2015 18:51:54 <local>}
\textbf{Renew Time: 2/23/2015 8:51:54 <local>}
\textbf{Session Key Type: AES-256-CTS-HMAC-SHA1-96}

\textbf{Client: test.user @ LAB.LOCAL}
\textbf{Server: ldap/win2k8-de.lab.local @ LAB.LOCAL}
\textbf{KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96}
\textbf{Ticket Flags 0x00000000 -> forwardable renewable pre_authent ok_as_delegate}
\textbf{Start Time: 2/16/2015 8:51:59 <local>}
\textbf{End Time: 2/16/2015 18:51:54 <local>}
\textbf{Renew Time: 2/23/2015 8:51:54 <local>}
```
Identity Theft Using Pass-the-Ticket Attack

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

Recommendations
- Disconnect the relevant computers from the network or move them to a safe location during the investigation: unknown processes, services, registry entries, unauthorized access, etc.
- Disable Grafnetter Michael's account

Resources (3)
- MTVMDC02 to CIFS
- MAINSTREAM.LOCAL to KRBTGT
- MTVMDC03 to CIFS
Demo
Pass-the-Hash Attack

```
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.

Maurenc Jaroslav
Delivery Manager

Maurenc Jaroslav... computer

NTLM hash

MAIN010NB

MTVMDC02

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.

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

<table>
<thead>
<tr>
<th>From</th>
<th>Accessed</th>
<th>Via Domain Controllers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Michael Dubinsky</strong></td>
<td><strong>Accessed (8)</strong></td>
<td></td>
</tr>
<tr>
<td>10:47 PM Wednesday March 25, 2015</td>
<td>Michael's-iPad</td>
<td>DC to KRBGTG</td>
</tr>
<tr>
<td>10:47 PM Thursday March 26, 2015</td>
<td>Michael's-iPad</td>
<td>DC to KRBGTG</td>
</tr>
<tr>
<td>11:37 PM Wednesday April 15, 2015</td>
<td>ExtVendor-PC</td>
<td>AORATO.COM to KRBGTG</td>
</tr>
<tr>
<td>11:59 PM Wednesday April 15, 2015</td>
<td>SharedAdmin-SRV</td>
<td>SharedAdmin-SRV to CIPS</td>
</tr>
<tr>
<td>11:59 PM Wednesday April 15, 2015</td>
<td>SharedAdmin-SRV</td>
<td>DC to KRBGTG</td>
</tr>
<tr>
<td>11:59 PM Wednesday April 15, 2015</td>
<td>Test-PC</td>
<td>DC to KRBGTG</td>
</tr>
<tr>
<td>11:59 PM Wednesday April 15, 2015</td>
<td>Finance-PC</td>
<td>DC to KRBGTG</td>
</tr>
</tbody>
</table>
Honeytoken

Administrator
Built-in account for administering the computer/domain
mainstream.local
Created on Jun 18, 2006
Administrator@mainstream.cz

Sensitive  Disabled  Locked

2 suspicious activities

Summary       Activities       Suspicious activities

Memberships (4)

- Domain Admins
  Designated administrators of the domain

- Group Policy Creator Owner
  Members of this group can modify group policy settings

- Domain Users
  All domain users

- Administrators
  Administrators have complete and un...
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.

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
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.

Recommendations
- Rejoin or remove the computers from the domain
Microsoft ATA Licensing Options
# Microsoft ATA Licensing

<table>
<thead>
<tr>
<th>License Type</th>
<th>Per user</th>
<th>Per OSE*/device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Through Enterprise CAL Suite per-user license</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Through Enterprise CAL Suite per-device license</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Through Enterprise Mobility Suite user subscription license</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Through Enterprise Cloud Suite user subscription license</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Standalone license - Open L&amp;SA estimated retail price, annualized**</td>
<td>USD $80</td>
<td>USD $61.50</td>
</tr>
</tbody>
</table>
# Enterprise CAL Suite

<table>
<thead>
<tr>
<th>Windows Server Active Directory Rights Management Services CAL</th>
<th>Exchange Server Enterprise CAL with Services</th>
<th>SharePoint Server Enterprise CAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skype for Business Server Enterprise CAL</td>
<td>Exchange Online Archiving for Exchange Server</td>
<td>Advanced Threat Analytics</td>
</tr>
<tr>
<td>Windows Server CAL</td>
<td>Exchange Server Standard CAL</td>
<td>SharePoint Server Standard CAL</td>
</tr>
<tr>
<td>Skype for Business Server Standard CAL</td>
<td>System Center Configuration Manager CML</td>
<td>System Center Endpoint Protection</td>
</tr>
</tbody>
</table>
Enterprise Mobility Suite

- Advanced Thread Analytics
- Azure AD Premium (incl. Multi-Factor Authentication)
- Microsoft Intune
- Azure RMS
- Azure RemoteApp
- Microsoft Identity Manager
## Enterprise Cloud Suite

<table>
<thead>
<tr>
<th>Office 365</th>
<th>EMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office 365 Pro Plus</td>
<td></td>
</tr>
<tr>
<td>Exchange Online</td>
<td></td>
</tr>
<tr>
<td>Lync Online</td>
<td></td>
</tr>
<tr>
<td>SharePoint Online</td>
<td></td>
</tr>
<tr>
<td>Yammer</td>
<td></td>
</tr>
<tr>
<td>System Center CM</td>
<td></td>
</tr>
<tr>
<td>Windows Server CAL</td>
<td></td>
</tr>
<tr>
<td>Azure Rights Management</td>
<td></td>
</tr>
<tr>
<td>Windows Intune</td>
<td></td>
</tr>
<tr>
<td>Azure AD Premium</td>
<td></td>
</tr>
<tr>
<td>Windows SA Per User</td>
<td></td>
</tr>
</tbody>
</table>
Idan Plotnik
@idanPlotnik
Surfer, Tech and Business Geek, Founder and CEO @Aorato, Now Director Group Manager @Microsoft Security Division

New York

Idan Plotnik Retweeted
Michael Graffnetter @MGraffnetter - 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
OMG! I'm in RFC!
tools.ietf.org/html/rfc7457#r...
Microsoft Advanced Threat Analytics

Mgr. Michael Grafnetter
Architect