

Bring Your Own Threat Intelligence (BYOTI)

Focus on what matters

Abbas Kudrati
APAC Chief Cybersecurity Advisor
Microsoft
Abbas.Kudrati@Microsoft.com
@askudrati



About me

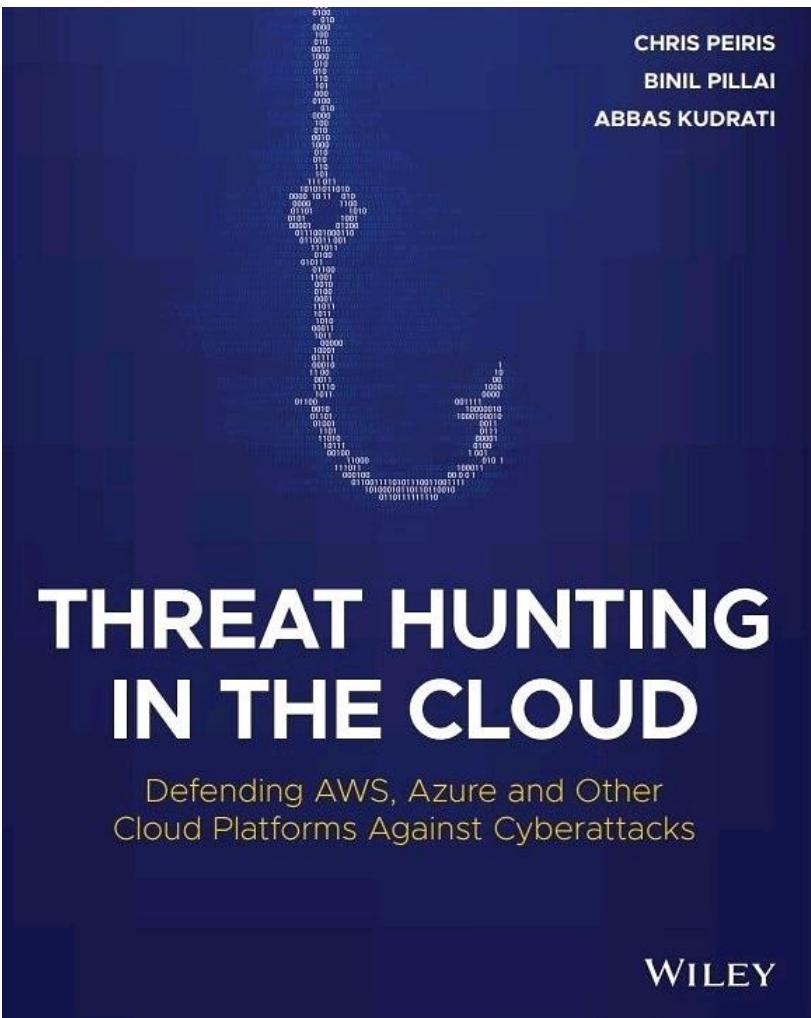
"You join Microsoft, not to be cool
but to make others cool"

Satya Nadella

- **Cybersecurity practitioner and CISO with 25 years of experience in Information / Cybersecurity.**
- **Part time Cybersecurity Professor with Deakin and LaTrobe University in Melbourne, Australia.**
- **Expertise in Zero Trust, Cybersecurity Strategy, Security Operations, Risk, Compliance, Cloud Security and Architecture.**



Upcoming books



Available on Amazon AU

Work in progress

**Zero Trust Journey
across the Digital
Estate**

By
**Abbas Kudrati &
Binil Pillai**



CRC Press
Taylor & Francis Group

Target release by May 2022.

Work in progress

**Digitization Risks in
Post Pandemic
World**

By
**Ashish Kumar,
Abbas Kudrati &
Shashank Kumar**



Target release by March 2022.

Navigating a shifting world

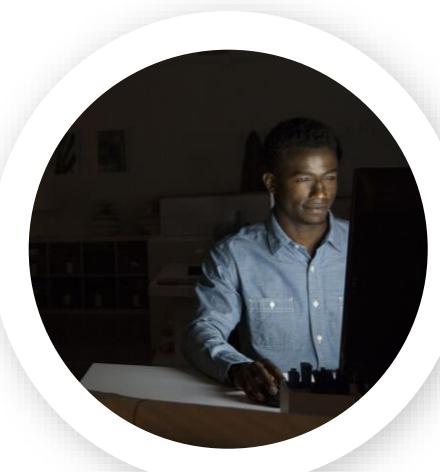
The nature of business
and work have changed



Conventional security
tools have not kept pace



Cost of breaches and
regulations are increasing



CYBERSECURITY TODAY impacts us all

A world map with a grid background. Overlaid on the map are several yellow dashed lines representing network traffic or data flow between various global locations. Superimposed on these lines are four large, semi-transparent blue circles, each containing a white icon. The first circle on the left contains a building icon. The second circle contains a user profile and document icon. The third circle contains a group of five people icon. The fourth circle on the right contains a calendar icon.

\$4 million

Average cost
of a data breach
in 2020

6 billion+

Records stolen by
hackers in 2019

1 million+

New malware
variants created
each day

101 days

Median # of days
between infiltration
and detection

Cybercrime has a supply chain, and a platform

The screenshot shows a website for "CENTRAL HACKER". On the left, there's a banner for "Ransomware solution" featuring a laptop with a lock screen. Below it, sections include "Who are we?", "We sell Ransomware", and "Failure is not an option". The main content area has a heading "HACKER FOR HIRE PRICING" and a sub-section "Hacker for Hire Services Pricing Sample". A table lists various hacking services with their prices and completion times. To the right, a sidebar titled "Dark Web Prices" lists items like Social Security (\$1), DDOS as a service (~\$7 per hour), and Exploits (\$1,000-\$300,000).

Services	Prices	Time to complete
Facebook Hacking	\$200-\$300	3-5 days
Email Hacking	\$200-\$300	3-5 days
SmartPhone Hacking	\$300-\$500	5-7 days
Website Hacking	\$500-\$2000	5-10 days
Database Hacking	\$500-\$2000	5-10 days
Special Hacking	\$500-\$5000	10 days
System Hacking	\$500-\$2000	5-10 days
Exploits	\$300-\$500	10 days

Dark Web Prices

Social Security	\$1
DDOS as a service	~\$7 per hour
Medical record	\$50 and up
Credit card data	\$0.25 to \$60
Bank account info	\$1,000 and up depending on the account type and balance
Mobile malware	\$150
Spam	\$50 for ~500,000 emails
Exploits	\$1,000-\$300,000
Maleware development	\$2,500 (Commercial malware)
Facebook account	\$1 for an account with 15 friends

[Russian Hydra DarkNet Market Made Over \\$1.3 Billion in 2020 \(thehackernews.com\)](https://thehackernews.com)

How do we combat this?

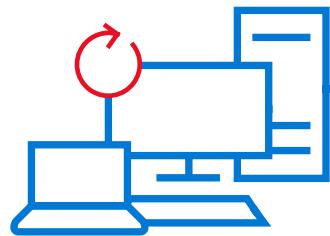
- Change of mindset?
- Strategies employed?

Designing for Failure – The Mindshift

THEN

Reliability:

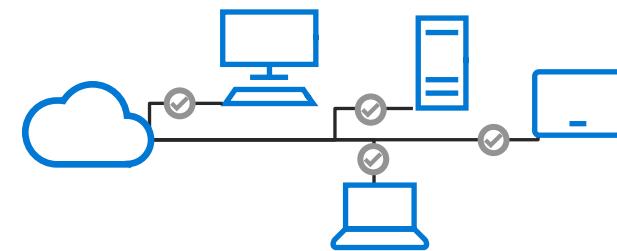
Designed not to fail



NOW

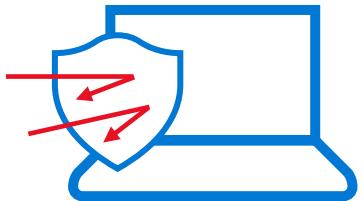
Resilience:

Designed to recover quickly



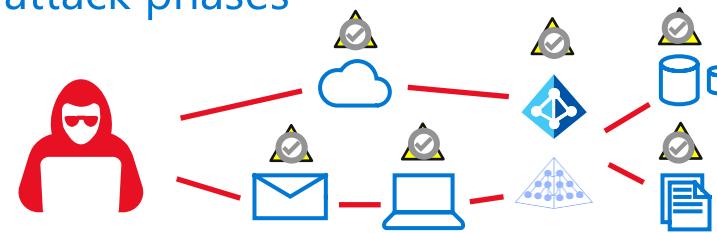
Prevent:

Every possible attack



Assume Compromise:

Protect, detect, and respond along attack phases



Strategies

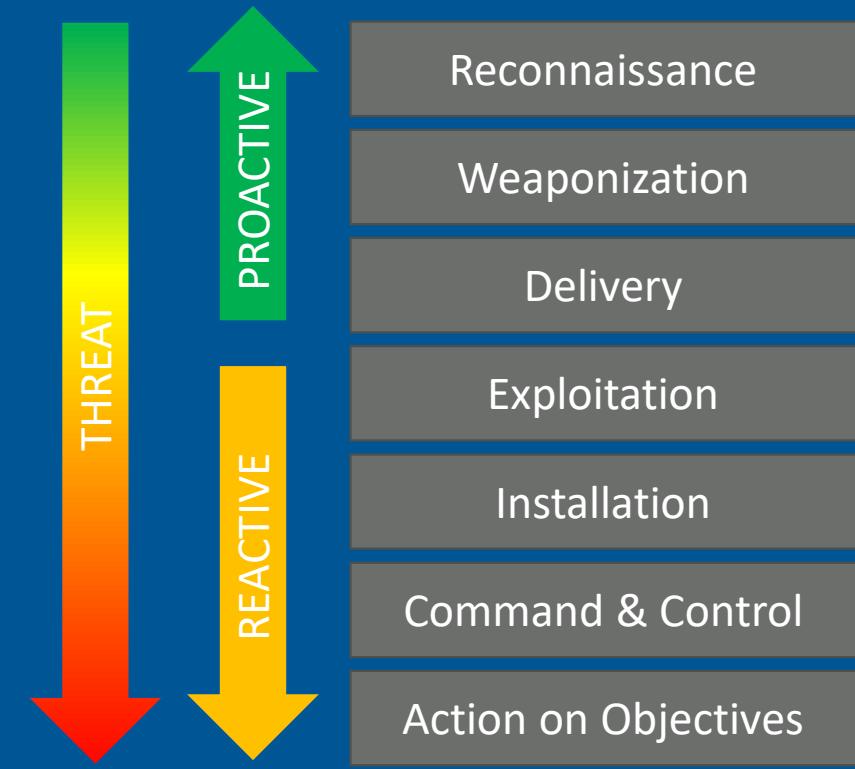
Defense-in-depth



Cybersecurity



Cyber Kill Chain



What is Threat Intelligence?

- Indicator of Compromise (IoC) is an artifact linked to a known vulnerability or attack.
- MITRE ATT&CK Framework describes tactics and techniques
- Common Vulnerabilities and Exposures ([CVE](#)) are publicly known cybersecurity vulnerabilities.
- The CVE List feeds the U.S. National Vulnerability Database ([NVD](#))
- The NVD documents fix information, severity scores, and impact ratings.

Closer look at Indicator of Compromises (IOC's)

- Indicator types include IP addresses, file hashes, domains, email addresses, & certificates
- IOC records often include an expiration date and confidence score in addition to the indicator value
- IOCs can reside in a local or remote database

Leveraging Threat Intel Spanning the Killchain



RECONNAISSANCE	WEAPONIZATION/ INFRASTRUCTURE SETUP	DELIVERY	EXPLOITATION	INSTALLATION	C2	ACTIONS ON INTENT
Detections submitted from multiple sensors	Threat Intelligence feeds and correlation data	Mail received by <ul style="list-style-type: none"> M. Smith (Sales) Detection <ul style="list-style-type: none"> Agenda.doc (Win32/NeroBlaze Dropper) 	IOA Detection <ul style="list-style-type: none"> Browser started suspicious process (Name: inst.dat) 	IOA Detection <ul style="list-style-type: none"> HOST: MSMITH-MAIL GoogleUpdate.EXE Rare Startup Program (Prevalence: 2 local /74 WW) 	ATA Detection <ul style="list-style-type: none"> HOST: MSMITH-MAIL PTH Detection ATA Detection <ul style="list-style-type: none"> HOST: DC-01 Mass Computer Enumeration 	Detection <ul style="list-style-type: none"> HOST: AZSQL-01 (Azure SQL instance) Mass download of database content from an unusual host
Offerings	INTERFLOW & THREAT ATTRIBUTION SERVICE	O365 ATP	WINDOWS DEFENDER ATP	WINDOWS DEFENDER ATP	ATA	AZURE SECURITY CENTER/ OMS
+ Content/Engage	Detection Dictionary Attribution report	Tactics, Techniques, and Processes (TTPs)	Related threats	Downloaded report/mitigation guidance	Engage Microsoft Cybersecurity Group	

What is a Threat Intelligence Provider?

- VirusTotal
- AlienVault
- Recorded Future
- EclecticIQ
- ThreatQuotient
- BlueVoyant
- Sixgill
- Palo Alto
- IBM Xforce
- FireEye
- MISP
- Anomali
- ThreatConnect
- Risk IQ

Threat perspectives

Organisation-specific Attack Based Threat Hunting

Hypothetical scenario

- Login to a cloud service from a non-corporate device to steal data

Predict and estimate the footprint

- Unusual IP/Machine name/OS/Geolocation/time/volume/authorisation failures/upload

Enact or hypothesise and gather artefacts

- Inspect logs, ID markers, registry

Block/Alert/Pass?

- CEO new phone? Attacker stealing data? Brute force attack?

Learnings

- Additional logs, if only we had blocked file downloads from new Geolocations

Why do customers need BYOTI?

- Assurance in the face of a major threat
- Compliance reasons
- Microsoft Threat Intelligence is not yet easy to validate (and for good reason!)

Threat Intelligence Challenges

How do we enable customers to gain visibility into rapidly changing threats while reducing the noise generated by insignificant events?



BYOIT Setup Options

- Manual Hunt / Analytics Rule
- Threat Intelligence Connector
- TAXII
- API (Logic App)



A structured language for cyber threat intelligence



A transport mechanism for sharing cyber threat intelligence



To protect customers and make the internet safer, our global security teams use machine learning to process:

- **Trillions** of raw security signals, which generates
- **Billions** of complex predictions and
- **Millions** of automated actions

Microsoft Threat Intelligence

Built on diverse signal sources and AI

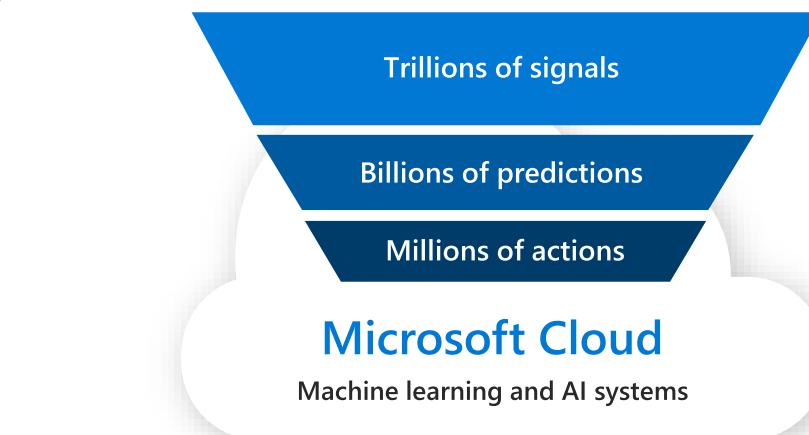
1.2B+
PCs, servers,
and IoT

URLs scanned
18M+

Emails
analyzed
470B+

iOS, macOS,
Android, Linux
and IoT devices

Documents scanned
600B+



Meeting
minutes delivered
4.1B+

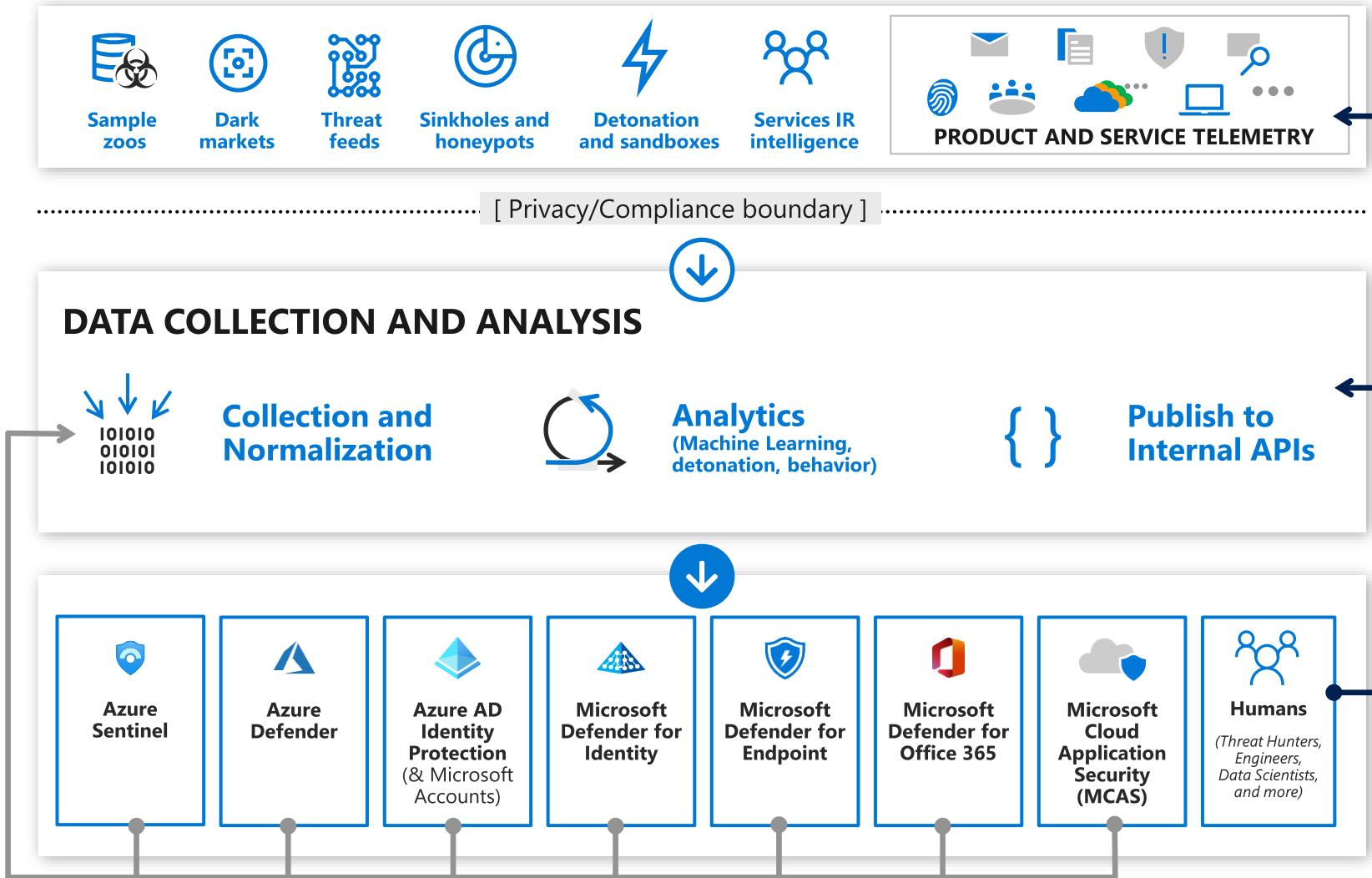
1.8PBs
Other clouds
and network logs

Identities
authenticated
630B+

Threats blocked
5B+

1B+
Apps and
service users

Inside View of Microsoft Threat Intelligence



- Products instrumented to strict privacy/compliance standards
See [Microsoft Trust Center](#)
- Analytics help fuel new discoveries
- Products make data available
- Products use Interflow APIs to access results
- Products generate data which feeds back into system
- Humans identify attacks, improve analytics, feed back into databases and product design

Customers want three things from Threat Intelligence:

- Protect them from known, relevant threats
- Insights that help them triage and prioritize.
- Understand the full context of threats before they are affected.

More relevant, accurate & actionable data.



Microsoft Threat Intelligence - Threat Analytics

Threat analytics

Latest threats

BazaLoader: Foothold for ransomware	0/0
Emotet breaks hiatus with spike in cybercrime activity	0/0
IcedID's frosty arrival can lead to data theft	0/0
Evolution and return of GravityRAT	0/0

High-impact threats ⓘ

Simulated threat	2/5
Adwind RAT lands using DDE	1/3
Cobalt Strike: Hiding in the red	0/3
AngelWind SQL mining	0/1

Threats summary

2/96 threats impact your organization

Legend: Devices with active alerts (red), Devices with resolved alerts (green), Threats with active impact (dark red), Threats with resolved impact (dark green), Threats with no impact (light gray), Threats with no alerts linked (gray)

Choose columns ▾

Threat	Devices with ale...	Devices with alerts in the last 7 d...	Published	Last updated	...
BazaLoader: Foothold for ransomware	0 active / 0	_____	1/30/21, 1:40 AM	1/30/21, 1:40 AM	...
Emotet breaks hiatus with spike in cybercrime activity	0 active / 0	_____	1/29/21, 1:24 AM	1/30/21, 1:24 AM	...
IcedID's frosty arrival can lead to data theft	0 active / 0	_____	1/29/21, 10:06 PM	1/29/21, 10:06 PM	...
Evolution and return of GravityRAT	0 active / 0	_____	1/29/21, 7:55 AM	1/29/21, 7:55 AM	...
Attackers phish for OAuth consent from remote workers	0 active / 0	_____	1/26/21, 1:35 AM	1/26/21, 1:35 AM	...
The Solorigate missing link	0 active / 0	_____	1/21/21, 8:07 PM	1/21/21, 8:07 PM	...
CVE-2020-10148 leads to trojanized SolarWinds binary	0 active / 0	_____	1/12/21, 2:05 AM	1/12/21, 2:05 AM	...

Microsoft Threat Intelligence - Threat Analytics Report

Threats > Sophisticated actor attacks FireEye

Overview Analyst report Mitigations

Executive summary

On December 8, 2020, FireEye disclosed that they were targeted by a highly sophisticated threat actor. The incident is an indication that no organization is safe from such sophisticated attacks – even security companies. FireEye disclosed the information on the attack so that the community will be better equipped to fight and defeat cyber-attacks.

In the initial disclosure on December 8, 2020, FireEye revealed that a highly sophisticated actor gained access to their red team tools used to test FireEye's customers' defenses. FireEye also provided technical details on those tools through a GitHub repository. In their statement, FireEye asked security vendors to detect the red team tools out of an abundance of caution. Microsoft has added protections per their request.

These red team tools are best detected through antivirus and behavioral offerings. Microsoft Defender antivirus, Microsoft Defender for Endpoint, Microsoft Defender for Office 365, and Exchange Online Protection provide detection for these tools. Antivirus and endpoint customers should keep antimalware products up-to-date. Customers utilizing automatic updates do not need to take additional action to receive these protections. Enterprise customers managing updates should select the new detection build (**1.329.63.0** or newer) and deploy it across their environments. The protections for our email offerings are already live and require no further action to be protected.

Microsoft does not have additional information beyond the public disclosure to share. This remains a fluid situation by a determined adversary that we are monitoring. As additional information becomes available, we will update customers through this threat analytics report.

Analysis

As stated earlier, the attacker targeted and accessed red team (also known as penetration testing) assessment tools that FireEye uses to test its customers' security.

Microsoft security researchers have investigated these tools to ensure robust detection coverage for the existing tools as well as possibly hacked and compromised versions. While there are some proprietary applications developed in-house by FireEye such as their GoLang-based remote access tool, most of these tools consist of open-source scripts and attack frameworks, with some being modified according to FireEye's use.

The open-source tools and attack frameworks that are included or referenced in the red team tools shared by FireEye include the following below.

- Cobalt Strike - commercial penetration testing and post-exploitation framework
- Inveigh - man-in-the-middle ADIDNS/LLMNR/NBNS/mDNS/DNS spoofing tool in PowerShell code
- Impacket - open-source Python-based scripts for achieving remote service execution and credential dumping
- Mimikatz - open-source application used to view and save credentials commonly used for credential stealing and escalating privileges
- PowerSploit - open-source framework based on PowerShell scripts used for remote code execution, defense evasion, persistence and exfiltration
- Pupy - open-source remote access and post-exploitation program
- Rubeus - toolset for raw Kerberos interaction and abuses
- SafetyKatz - modified Mimikatz
- SharpZeroLogon - exploit kit for CVE-2020-1472 or the NetLogon Elevation of Privilege vulnerability

Most of these applications have already been reported in detail with detection coverage and mitigations in previous Threat Analytics articles such as:

- [Cobalt Strike: Hiding in the Red](#)
- [Hunting for PowerShell Empire](#)

Microsoft Threat Intelligence - Threat Analytics

Threat analytics

Latest threats

BazaLoader: Foothold for ransomware	0/0
Emotet breaks hiatus with spike in cybercrime activity	0/0
IcedID's frosty arrival can lead to data theft	0/0
Evolution and return of GravityRAT	0/0

High-impact threats

Simulated threat	2/5
Adwind RAT lands using DDE	1/3
Cobalt Strike: Hiding in the red	0/3
AngelWind SQL mining	0/1

Threats summary

2/96 threats impact your organization

Legend:

- Devices with active alerts
- Devices with resolved alerts
- Threats with active impact
- Threats with no impact
- Threats with resolved impact
- Threats with no alerts linked

Choose columns

Threat	Devices with ale...	Devices with alerts in the last 7 d...	Published	Last updated	...
BazaLoader: Foothold for ransomware	0 active / 0	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>	1/30/21, 1:40 AM	1/30/21, 1:40 AM	
Emotet breaks hiatus with spike in cybercrime activity	0 active / 0	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>	1/29/21, 1:24 AM	1/30/21, 1:24 AM	
IcedID's frosty arrival can lead to data theft	0 active / 0	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>	1/29/21, 10:06 PM	1/29/21, 10:06 PM	
Evolution and return of GravityRAT	0 active / 0	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>	1/29/21, 7:55 AM	1/29/21, 7:55 AM	
Attackers phish for OAuth consent from remote workers	0 active / 0	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>	1/26/21, 1:35 AM	1/26/21, 1:35 AM	
The Solorigate missing link	0 active / 0	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>	1/21/21, 8:07 PM	1/21/21, 8:07 PM	
CVE-2020-10148 leads to trojanized SolarWinds binary	0 active / 0	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>	1/12/21, 2:05 AM	1/12/21, 2:05 AM	

Microsoft Threat Intelligence - Threat Analytics Mitigations

Microsoft Defender Security Center

User Search Microsoft Defender for Endpoint MTPGlobalReader@mtpde...

Threats > Sophisticated actor attacks FireEye

Overview Analyst report Mitigations

Secure configuration status ①

28 misconfigured devices

Exposed Secure Unknown Not applicable

Vulnerability patching status ①

2 vulnerable devices

Exposed Secure

Mitigation details

Secure configuration

Product/Component	Settings/Updates	Exposed devices
Security controls (Antivirus)	Turn on real-time protection	1
Security controls (Antivirus)	Enable cloud-delivered protection	1
Security controls (Antivirus)	Update Microsoft Defender Antivirus definitions to version 1.329.63.0 or later	5
Security controls (Attack Surface Reduction)	Block execution of potentially obfuscated scripts	27
Security controls (Attack Surface Reduction)	Block executable content from email client and webmail	27
Security controls (Attack Surface Reduction)	Block JavaScript or VBScript from launching downloaded executable content	27
Security controls (Attack Surface Reduction)	Block untrusted and unsigned processes that run from USB	27



Where does Microsoft publish
threat intelligence !

Where does Microsoft publish threat intelligence

- Global Threat Activity
- Microsoft Digital Defense Report Report
- Microsoft Defender for Endpoint
 - Microsoft Threat Experts
- Microsoft Detection and Response Team



Microsoft Worldwide Security Intelligence provides a macro level view of the top threats to enable monitoring and analysis of high-volume events occurring in real time.



Explore the world from your desktop—one photo at a time. Get the Bing Wallpaper app today.

No thanks

Get it now



Microsoft Security Intelligence

Threats Blogs Downloads ▾ Submissions ▾ Help ▾

All Microsoft ▾



All Microsoft

1

Search the threat encyclopedia



Global threat activity

Countries or regions with the most malware encounters in the last 30 days

Select a region



Worldwide

88,999,509 devices with encounters

Top threats:

HackTool:Win32/AutoKMS
HackTool:Win64/AutoKMS
HackTool:MSIL/AutoKms
HackTool:Win32/Keygen
Trojan:Win32/CryptInject!ml

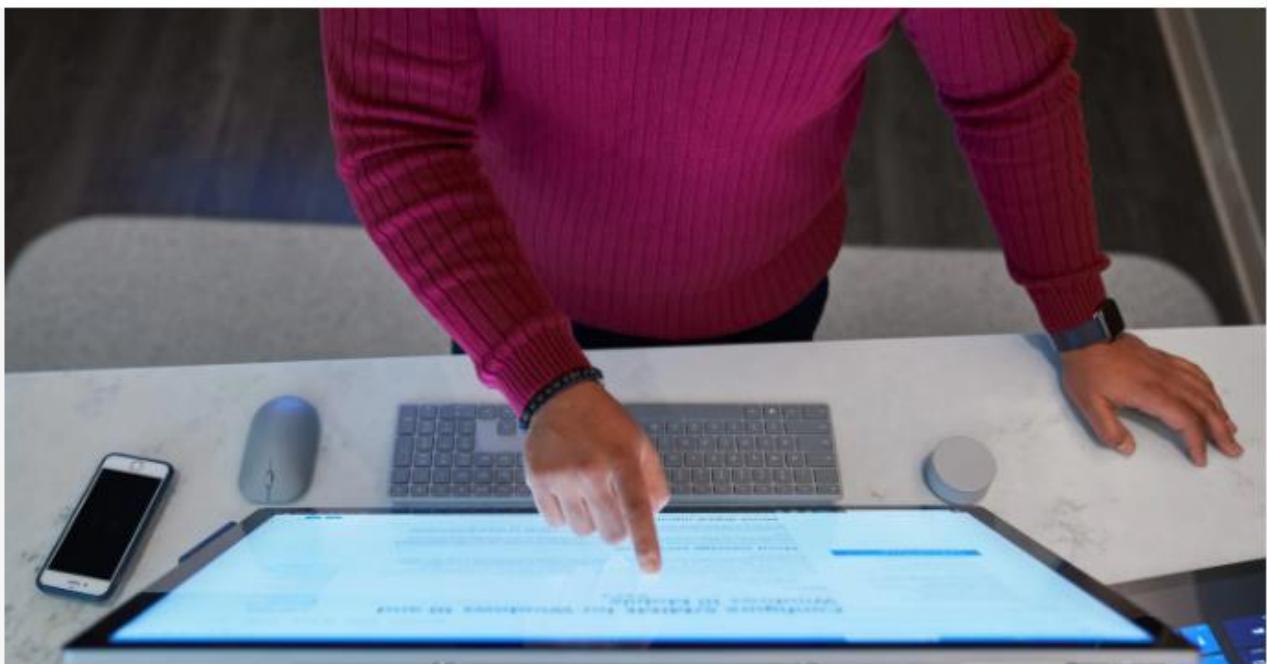
**Microsoft Digital Defense Report provides global insights
about threat intelligence from experts, practitioners and
defenders at Microsoft.**



Microsoft Digital Defense Report

Get the latest insights about the threat intelligence landscape and guidance from experts, practitioners, and defenders at Microsoft.

[Download the report](#)



Informed by over 8 trillion daily security signals and observations from our security and threat intelligence experts, our new Digital Defense Report presents telemetry and insights about the current state of cybersecurity.

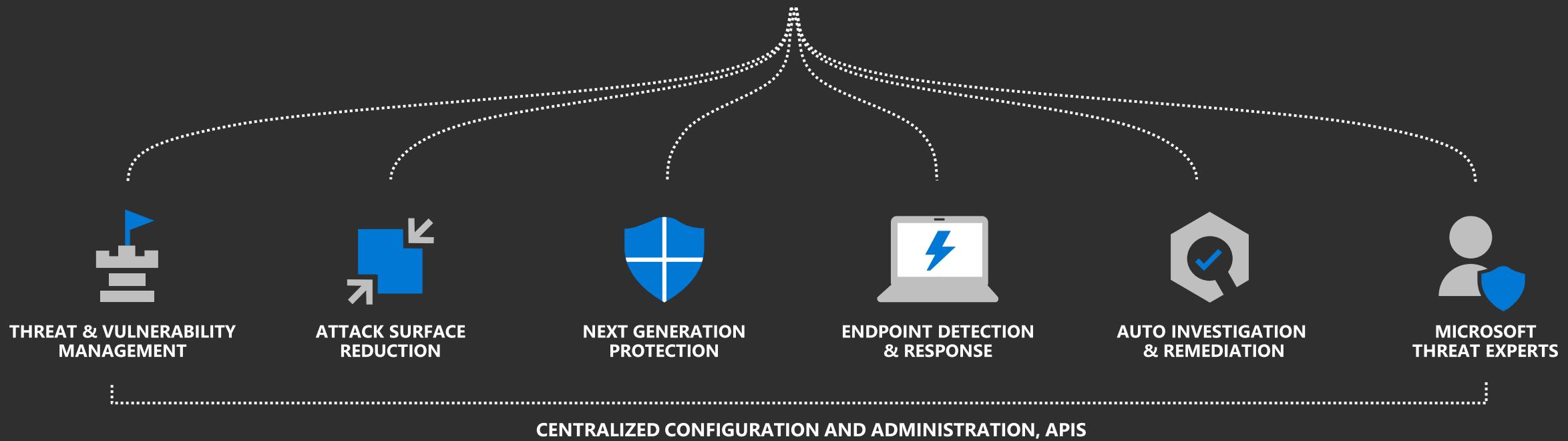
Download archived security

Microsoft Defender for Endpoint provides your Security Operations Centers with technical capabilities to monitor, investigate and respond to risks and threats across your technical landscape.



Microsoft Defender For Endpoint

Built-in. Cloud-powered.



Threat Analytics

See how you do against major threats

<https://securitycenter.microsoft.com>

Threat to posture view

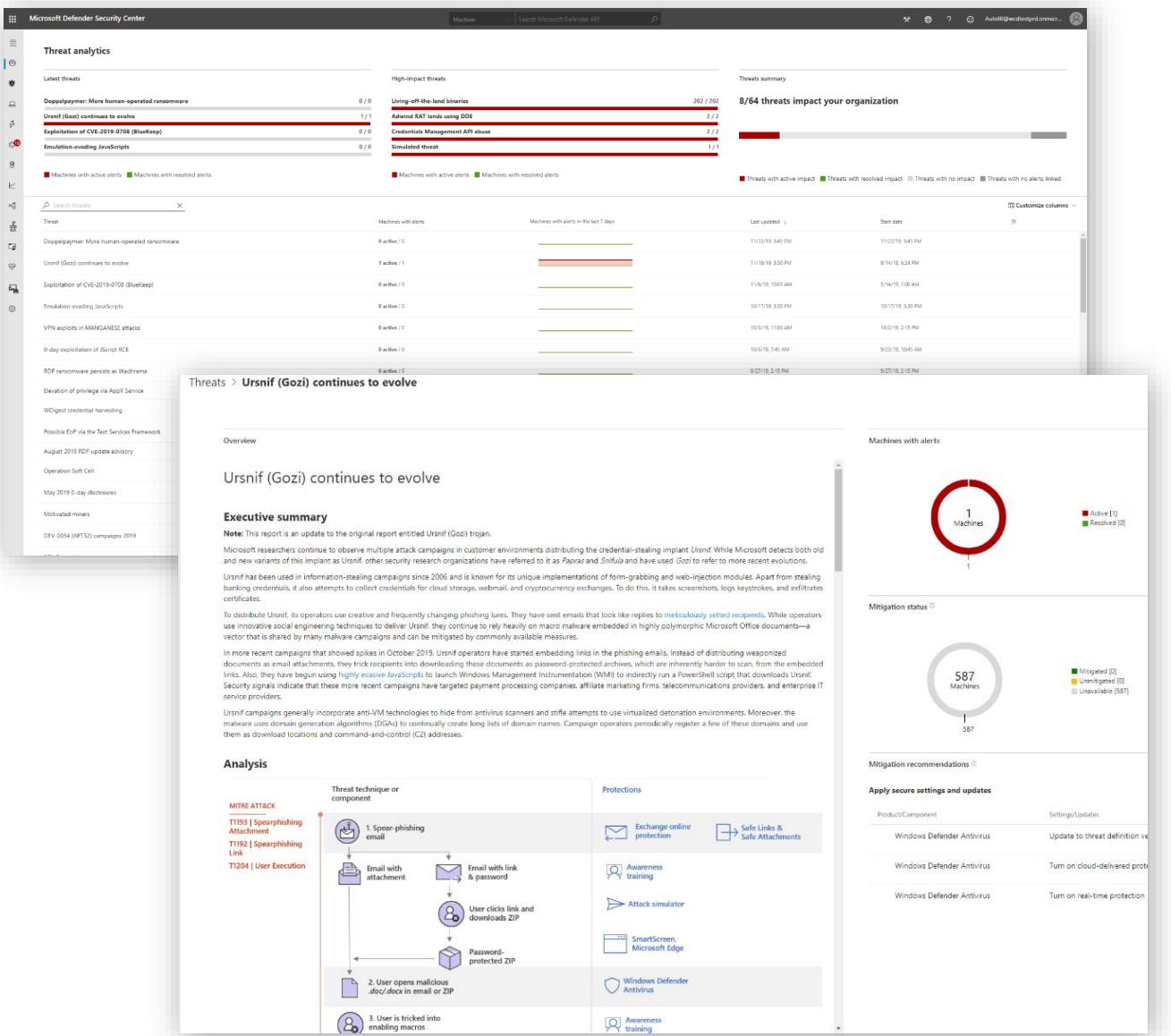
See how you score against significant and emerging campaigns with interactive reports.

Identify unprotected systems

Get real-time insights to assess the impact of the threat on your environment.

Get guidance

Provides recommended actions to increase security resilience, to prevention, or contain the threat.



https://securitycenter.windows.com/threatanalytics3

Microsoft Defender Security Center

Threat analytics

Device Search Microsoft Defender ATP

Latest threats

Threat	Count
ELBRUS (FIN7) activity group	0/0
Signature spoofing exploit with MSI or CAT headers	0/0
CVE-2020-1472 Netlogon EoP vulnerability	0/0
Print Spooler EoP: Persistence pays off	0/0

High-impact threats

Threat	Count
Simulated threat	2/7
Adwind RAT lands using DDE	1/5
Cobalt Strike: Hiding in the red	0/5
Credentials Management API abuse	0/1

Threats summary

2/80 threats impact your organization

Legend:

- Devices with active alerts (Red)
- Devices with resolved alerts (Green)
- Threats with active impact (Red)
- Threats with resolved impact (Green)
- Threats with no impact (Grey)
- Threats with no alerts linked (Grey)

Threat	Devices with alerts	Devices with alerts in the last 7 days	Last updated	Start date
ELBRUS (FIN7) activity group	0 active / 0	0	10/14/20, 7:30 AM	10/14/20, 7:30 AM
Signature spoofing exploit with MSI or CAT headers	0 active / 0	0	10/13/20, 8:15 AM	8/11/20, 8:00 AM
CVE-2020-1472 Netlogon EoP vulnerability	0 active / 0	0	10/5/20, 3:35 PM	8/11/20, 8:00 AM
Print Spooler EoP: Persistence pays off	0 active / 0	0	10/5/20, 11:50 AM	10/5/20, 11:50 AM
Adwind utilizes Java for cross-platform impact	0 active / 0	0	9/8/20, 9:50 AM	9/8/20, 9:50 AM
BISMUTH: Mining for intelligence and coins	0 active / 0	0	9/3/20, 7:40 AM	9/3/20, 7:40 AM
CHIMBORAZO: StrangeU infra marks 2020 attacks	0 active / 0	0	8/25/20, 2:08 PM	8/24/20, 9:35 AM

Customize columns

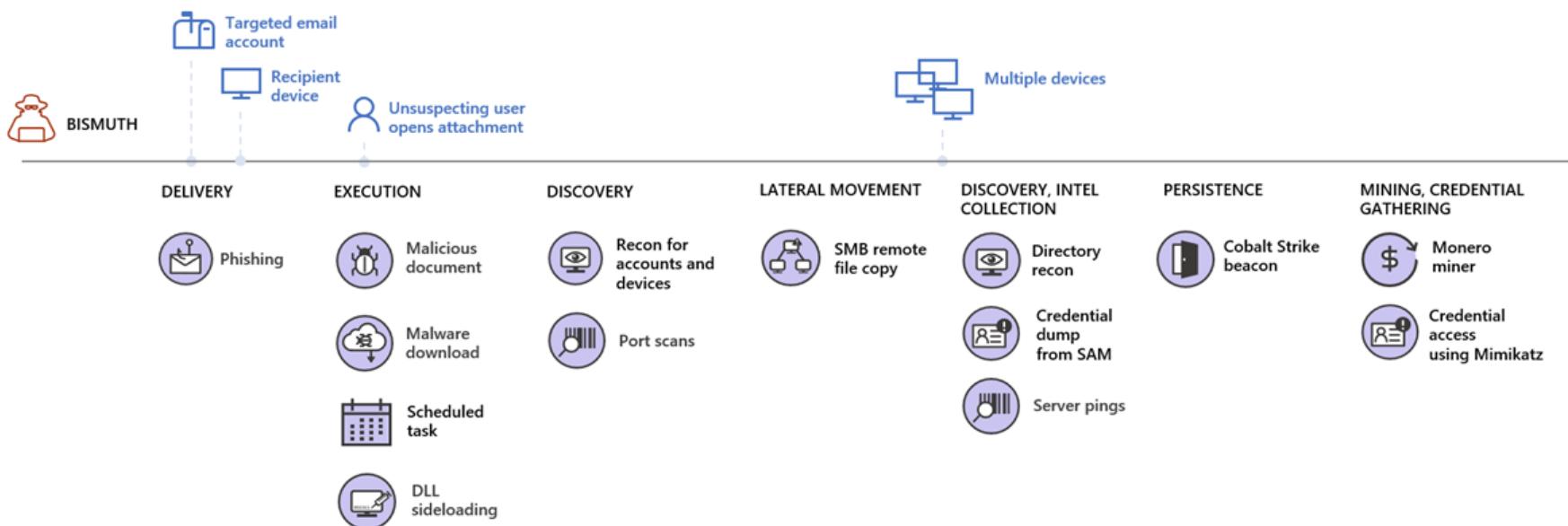
Need help?

Threats > **BISMUTH: Mining for intelligence and coins**

Overview Analyst report Mitigations

Analysis

BISMUTH stayed true to form using tactics, techniques, and procedures known to be associated with the group, including their use of Cobalt Strike in different stages as well as sideloading of malicious DLLs using Word 2007. During these attacks, however, they also exhibited new, sophisticated behaviors and activities. For example, the attacks co-opted antivirus programs to connect to Cobalt Strike beacons, used a debugger to inject Windows processes with Base64-encoded Mimikatz commands, and even mined for Monero coin—an activity that isn't commonly associated with nation-state actors.

**Delivery**

BISMUTH gained initial access by sending specially crafted malicious emails from a Gmail account that appears to have been made specifically for this campaign. It is likely the group conducted reconnaissance using publicly available sources and chose individual targets based on their job function. Each email went to only one recipient at each organization and used tailored subject lines and lure themes:

- Dự thảo hợp đồng (translates from Vietnamese to "Draft Contract")
- Ứng tuyển - Trưởng ban nghiên cứu thị trường (translates from Vietnamese to "Application form - Head of Market Research")

While the group sent numerous phishing emails, most recipients did not open the malicious Microsoft Word attachments. Unfortunately, it only took one user at each affected organization opening the malicious attachment to enable BISMUTH to establish a foothold in the organization. Of note, the group sent several replies to one of these emails, which can indicate that they corresponded with some targets before convincing them to open attachments and inadvertently launch the payload.

Execution through a malicious .doc and DLL sideloading

Upon opening of the malicious .doc file, WinWord.exe dropped several files in the hidden ProgramData folder: *MpSvc.dll*—a malicious DLL with the same name as a legitimate Microsoft Defender Antivirus DLL—and a copy of *MsMpEng.exe*, the legitimate Microsoft Defender Antivirus executable. The malicious document then added a scheduled task that launched the *MsMpEng.exe* copy and sideloaded the malicious *MpSvc.dll*. While the latest version of Microsoft Defender Antivirus is not susceptible to DLL hijacking, BISMUTH used older versions of the application to deliver their payload.

Need help?

Microsoft Threat Experts provide your Security Operations Centers with deep knowledge, expert level monitoring, analysis, and support to identify critical threats in your unique environment.

Managed Hunting by Microsoft Threat Experts

An additional layer of monitoring and analysis to help ensure that critical threats don't get missed



Targeted attack notifications

We have your back.

Threat experts provide special insights and analysis that help ensure that the most critical threats are identified and responded to quickly and accurately.

Experts on demand

World-class expertise at your fingertips.

Threat experts from Microsoft provide technical consultation on relevant detections and adversaries.



Microsoft Threat Experts

Microsoft brings deep knowledge and proactive hunting to your Security Operations Center



THREAT MONITORING AND ANALYSIS

Reduce attacker dwell time and risk to business



HUNTER-TRAINED ARTIFICIAL INTELLIGENCE

Discover and prioritize attacks both known and unknown



PROACTIVE NOTIFICATION SERVICE

Expert hunters look deeper to expose human adversaries and advanced threats



FULL CONTEXT OF BREACH

Improve SOC response with specific info about scope and methods of entry



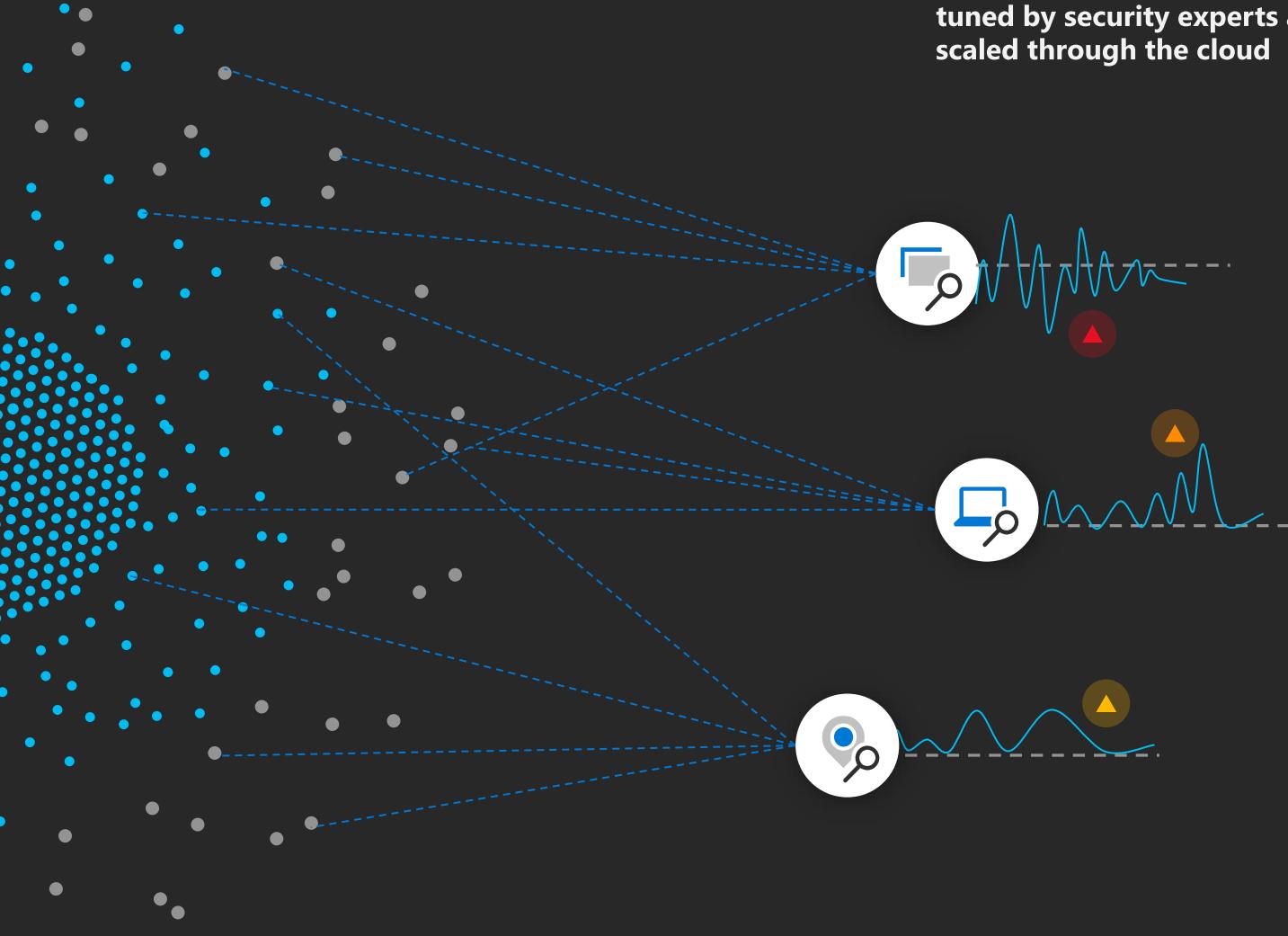
EXPERTS ON DEMAND

Partner with world-class security experts to better understand threats and alerts

Targeted attack notifications

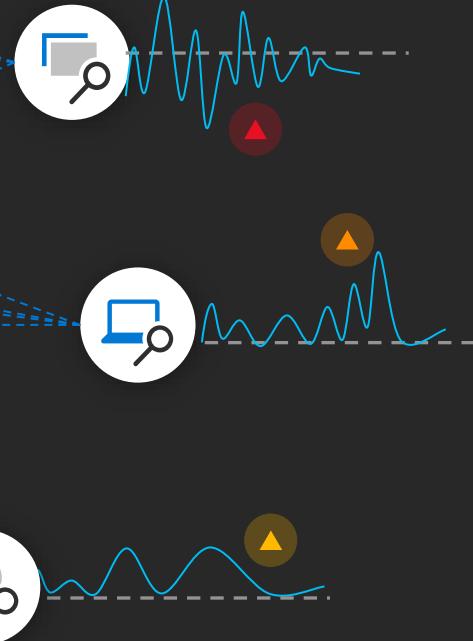
Intelligent Security Graph

Trillions of signals with unique insights



AI modules

Fine-grained self-learning modules,
tuned by security experts and
scaled through the cloud

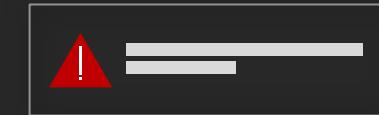


Managed alerts

AI modules prioritize anomalies
for hunters to investigate and
surface as targeted attack
notifications



MICROSOFT THREAT EXPERTS



Microsoft Threat Experts

New alert from Microsoft Threat Experts: Targeted Attack Behaviors and Data Exfiltration Observed

Microsoft Threat Experts

11:15

New alert from Microsoft Threat Experts: Targeted Attack...



Microsoft Defender ATP New Alert from Microsoft Threat Experts

Alert title

Targeted Attack Behaviors and Data Exfiltration Observed

Severity

High

Activity time

First Jul 03,2018 9:26:22 AM
Last Jul 03,2018 9:29:45 AM

Alert description

Malicious activity originating from a software supply chain compromise affecting the UltraEdit text editor software has been observed in your network.

- The activity involves credential theft and lateral movement, indicating a human adversary attempting to move throughout the network.
- Given the prevalence of UltraEdit in your network and only a limited number of machines affected, we believe the attacker has chosen to target specific machines within your organization.
- Based on the observed behavior, attacker's motivation is corporate espionage and data theft.

An unsigned payload is being dropped to \Device\HarddiskVolume2\Program Files\UltraEdit\ue.exe by the signed UltraEdit update process IDMUpdate.exe.

Suggested Queries

ProcessCreationEvents

```
| where EventTime > ago(30d)  
| where ProcessCommandLine startswith "schtasks.exe" /create /SC ONCE /TN Troj'  
| where InitiatingProcessFileName =~ "powershell.exe"
```



To prevent further impact, we recommend the following immediate actions:

- Confirm that this was indeed a small pen test on whether WDATP sensor could be stopped.
- Confirm that UserPII_adfb3256ed4b056b7921881468ac087d8aa64878 is in a role where this is expected behavior.

[Investigate in the portal](#)



[Privacy Statement](#)

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052



Incident alerts - Windo X +

https://securitycenter.windows.com/incidents/9724/alerts

Microsoft Defender Security Center

Incidents > 9724

9724

Edit name

Status
Active

Assigned to
Unassigned

Severity
High

Classification
(Not set)
Set status and classification

Categories
Suspicious Activity
Installation
Exploit

ACTIVE

Activity time
First - Jan 17, 2019, 1:55:26 PM
Last - Jan 21, 2019, 12:45:35 PM

Comments and History Actions and assistance

Alerts (4) Machines (2) Investigations (1) Evidence Graph beta

Threat Experts Targeted Attack Behaviors and Data Exfiltration Observed

Unexpected behavior observed by a process run with no command line arguments

EAF violation blocked by exploit protection

Suspicious process injection observed

Manage alert

Status Resolved

Classification Select classification...

Alert details

Severity High

Incident 9724

Category Suspicious Activity

Detection source Threat experts

Generated on Jan 17, 2019, 11:18:06 PM

First activity Jan 17, 2019, 1:55:26 PM

Last activity Jan 17, 2019, 1:55:26 PM

Assigned to analyst@contoso.com

Executive Summary

An advanced attack initiated from a successful phishing email launched by a user has been observed on two machines within your organization. From our preliminary investigation, two users opened emails with a malicious PDF file that caused the default browser to navigate to a malicious domain that then created a decoy PDF and a malicious DLL, which then communicated to a command and control server.

Go to alert page to see full description

ATTACKS SPAN EMAIL, IDENTITY, ENDPOINT and CLOUD

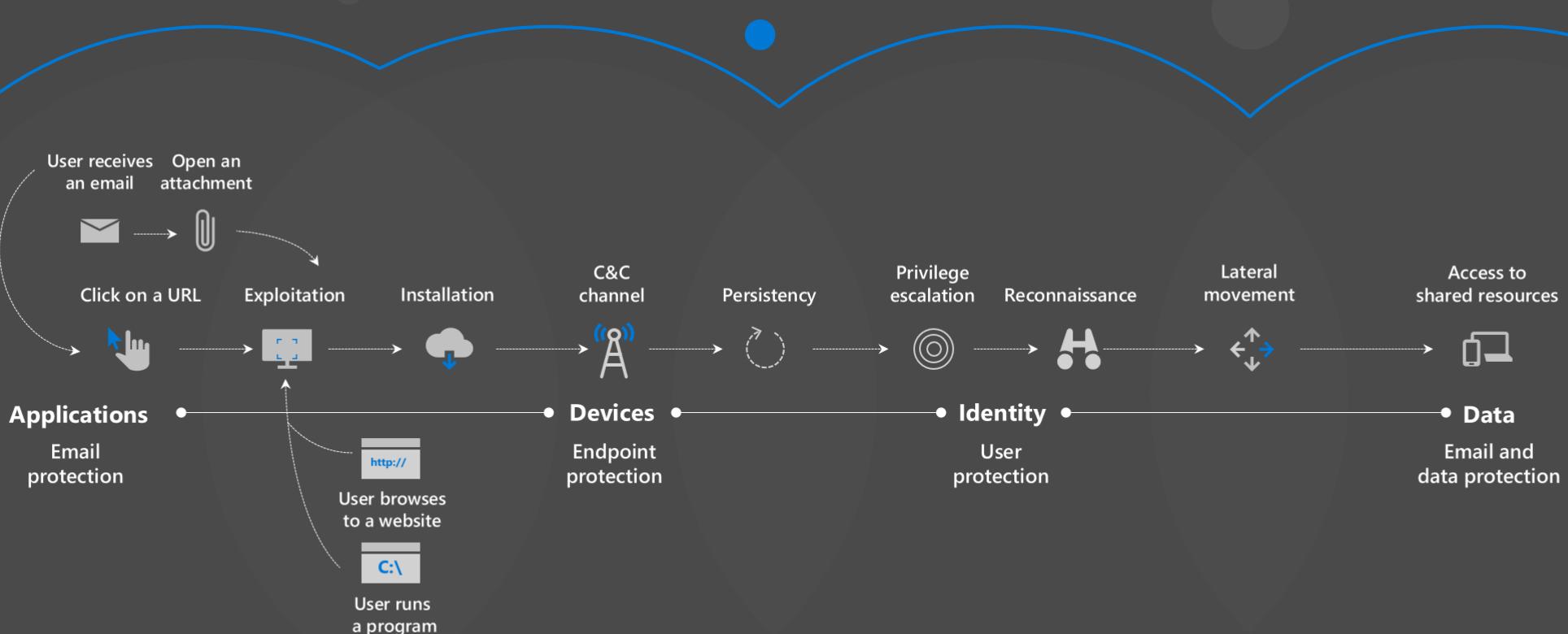


Figure 1 – Protecting the perimeter - An attack traverses the perimeters defended by M365 threat protection - Applications protected by Office 365 ATP and MCAS, Devices protected by Microsoft Defender ATP, Identities protected by Azure ATP and hybrid data centers protected by Azure Security Center

MITRE ATT&CK Simulations w/ MTE

Phase 1 attack steps	Coverage MDATP	Coverage w/ MTE
Initial Access: Red Team emulates a user phish on foothold machine where a user clicks on a self-extracting file which in turn extracts a batch file. This batch file opens a C2 channel to the attacker machine and establishes persistence using the "Startup" folder.	Alerts & Telemetry	Alerts & Telemetry
Initial Discovery: Red Team performs discovery on the local machine	Alerts & Telemetry	Alerts & Telemetry
Privilege Escalation: Red Team uses token duplication to escalate privilege on foothold machines	Alerts & Telemetry	Alerts & Telemetry
Discovery of Lateral Movement: Red Team performs further local and network discovery from foothold machine	Telemetry	MTE Included
Credential Access: Red Team performs credential dumping and steals token	Alerts & Telemetry	Alerts & Telemetry
Lateral Movement: Red Team uses stolen credentials to RDP to a server on the network	Telemetry	MTE Included
Persistence: Persistence is established on the server by adding a new admin user "Jesse" and by scheduling a malicious executable in Scheduled Tasks	Alerts & Telemetry	Alerts & Telemetry
Collection: Red Team performs file discovery on a server and logs keystrokes and captures screen for logged on user "Debbie"	Alerts & Telemetry	Alerts & Telemetry
Exfiltration: Red Team exfiltrates a Microsoft Office Visio file from the server via the foothold machine	None	MTE Included
Execution of Persistence: Red Team activates persistence (from step 7) by logging out and back in using the new admin account "Jesse"	Telemetry	MTE Included

Phase 2 attack steps	Coverage MDATP	Coverage w/ MTE
Initial Access: This stage is a continuation from Phase 1. Red Team uses credentials for user "Bob" to RDP into "CodeRed" and launch a PowerShell Empire payload "launcher.vbs"	Alerts & Telemetry	Alerts & Telemetry
Initial Discovery: Red Teams performs discovery on the local machine and on the network (Active Directory)	Alerts & Telemetry	Alerts & Telemetry
Privilege Escalation: Red Team escalates privilege using token manipulation	Alerts & Telemetry	Alerts & Telemetry
Discovery of Lateral Movement: Red Team performs LDAP queries to identify possible server targets	Telemetry	MTE Included
Credential Access: Red Team steals credentials using the keylog module and extracts passwords from a file stored remotely on "Conficker"	Alerts & Telemetry	Alerts & Telemetry
Lateral Movement: Red Team attempts to brute force admin shares on several machines and then performs a network log on to \$Admin share to "Conficker" using account "KMitnick". Red Team also compromises "Creeper" and runs a vbs payload on it and establishes persistence on "Creeper" using a Windows Service	Alerts & Telemetry	Alerts & Telemetry
Persistence: Red Team establishes persistence on "Creeper" by modifying file permission and by manipulating accessibility feature (magnify.exe)	Alerts & Telemetry	Alerts & Telemetry
Collection: Red Team performs file discovery on "Conficker" and copies a .vsdx from there to "CodeRed"	Telemetry	MTE Included
Exfiltration: Red Team performs exfiltration on "CodeRed" over FTP	Telemetry	MTE Included
Execution of Persistence: Red Team activates persistence by logging through RDP to "Creeper" and activating the "Magnifier" accessibility tool to run as LOCAL SYSTEM	Alerts & Telemetry	Alerts & Telemetry

Experts on demand

Experts on Demand - Overview

What it is:

**On-demand support for Microsoft Defender alerts,
suspicious activity, and threat intelligence**

What it's not:

Product support → Premier Support (CSS)

Testing guidance → Account Representative

Incident response → Microsoft Detection and Response



Incident alerts - Windo X +

https://securitycenter.windows.com/alert/636833638868580114_-144490119

Microsoft Defender Security Center

Search (File, IP, URL, Machine, User)

analyst@contoso.com

Incidents > 9724 > Targeted Attack Behaviors and Data Exfiltration Observed

Targeted Attack Behaviors and Data Exfiltration Observed

This alert is part of incident (9724) Threat Experts

Automated investigation is not applicable to alert type

Alert context

omkantor-7050
contoso\omkantor

First activity: 01.17.2019 | 13:55:26
Last activity: 01.17.2019 | 13:55:26

Ask a Threat Expert Resolved
Classification: Not set
Assigned to: analyst@contoso.com

Windows Defender ATP guide
Microsoft support
Microsoft premier support
License
Simulations & tutorials

Actions

Severity: High
Category: Suspicious Activity
Detection source: Threat experts

1

Description

Executive Summary

An advanced attack initiated from a successful phishing email launched by a user has been observed on two machines within your organization. From our preliminary investigation, two users opened emails with a malicious PDF file that caused the default browser to navigate to a malicious domain that then created a decoy PDF and a malicious DLL, which then communicated to a command and control server.

We recommend further investigation and actions be taken immediately in response to this threat.

Timeline of Observed Events

A breakdown of key events from the attack on the compromised machines is as follows:

- (11/14/2018 9:59 AM UTC) User opened email in Outlook that contained the malicious PDF, which then causes the default browser to connect to a malicious domain and makes the browser create a .LNK and .ZIP file.
- (11/14/2018 9:59 AM UTC) PowerShell opens the LNK and then creates the malicious payload utilizing Cobalt Strike, cyzfc.dat. PowerShell also creates a decoy PDF with the same name as the one opened in the email and launches it in AcroRd32.exe to make the user believe that the PDF was opened as expected.
- (11/14/2018 9:59 AM UTC) PowerShell launches rundll32.exe which loads the cyzfc.dat payload, which connected to a malicious command and control server on port 443.

Alert process tree

Recommended actions

Queries

This query will surface the compromised user for easier investigation on the entry point machine

```
ProcessCreationEvents | where EventTime between (datetime(11/14/2018 09:59:05)..datetime(11/14/2018 09:59:06)) and MachineId == "0b8b67d65e2912ac569894180dc82d3805880bd7"  
| project AccountSid
```



Threat Intelligence Updates

- Sentinel: New Threat Intelligence Analytic Rule
- Sentinel: New Microsoft Threat Intelligence Connector
- M365 Defender: Network Protection Added Coverage (MacOS, Android etc.)

Takeaways

- Use proactive Threat Hunting for incident management and further assurance
- Create organization specific hypothesis for threat hunting.
- Enroll into Advance security capabilities in Microsoft 365 services.
- Enable features like Network Protection, Cloud Protection, Block at First Sight
- Use Playbooks in Sentinel to automate Threat Hunting into M365 products such as Defender for Endpoint.

“Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win”

~ John Lambert (Microsoft)



Thank You!

