Cyberspace and Guerilla Warfare
Carbon Black Research
Global Cyberattacks Origins

1. China
2. Russia
3. North Korea
4. USA
5. Iran
Hidden Cobra

Dramatic evolution of capabilities due to tech transfer from Russia.

HIDDEN COBRA actors are using malware variants in conjunction with proxy servers to maintain a presence on victim networks and to further network exploitation.

Use custom binary protocol to beacon back to command and control via TCP port 8080 or 8088 some use SSL.

GRAFTOR: Customizable fileless malware with multiple variants
Offense Must Inform Defense: The IRTR
Island Hopping Occurs 50% of the Time
3 Forms of “Island Hopping”

- Network-based “island hopping”
- Website converted into a “watering hole”
- Reverse Business Email Compromise
Access Mining Marketplaces
Login Form

UAS RDP SHOP #1

Login:

Password:

[get new]

captcha

Register new account

Enter

TOR Link

CARDING HACKING

TRUMP'S DUMPS

LARGE BASE & LOW PRICE

ENJOY AND MAKE MONEY HERE

PRIVATE CREDIT SERVICE
Access Mining

Primary Infection Vector:
EternalBlue Scanning and Exploitation

Tertiary Infection Vectors:
Drive-by Downloads
Watering-Hole Attacks
Phishing

Invoke persistence via WMI
Download lbt.txt
Download up.txt

Nodes Added to Botnet
Remote Access Marketplaces
High Value Assets Identified

Data migrated off to second stage server

Kill processes listed in lbt.txt

Download and execute s.ps1
Download and execute lbt.txt

Data Uploaded to FTP Middleman Server

Collects host information and credentials
Uploads data to FTP server

Download and execute up.txt
Access Mining

Primary Infection Vector: EternalBlue Scanning and Exploitation
Tertiary Infection Vectors: Drive-By Downloads Watering Hole Attacks Phishing

Collects host information and credentials
Uploads data to FTP server

Invoke persistence via WMI
Download I.txt
Download up.txt

Download and execute I.txt
Download and execute s.txt

Download and execute up.txt

Credentials / RAT for Sale
Cybercriminals
Notes Added to Botnet
Remote Access Marketplaces
Data Uploaded to FTP Middleman Server
Kill processes listed in I.txt
Data migrated off to second stage server
High Value Assets Identified
PowerShell Data Collection

- Obtain External IP
- List Processes
- OS Fingerprinting
- Calculate Memory Capacity
- List CPU Info and Load %
PowerShell Credential Theft & Data Exfiltration

- **PowerSploit Mimikatz**
- **Write Data to File**
- **Plain Text Creds...**
- **Upload Data via FTP**
Over 100k unique infections identified in 1-week on a single FTP server

Over 500k unique infections known
70% witnessed LATERAL MOVEMENT
Living off the Land
40% of incident response professionals see instances of SECONDARY C2 being used on a sleep cycle during IR engagements.
56% Observe Counter IR
Steganography Makes a Comeback

VeryMal
Gandcrab
Zerp
Triton

Sundown Exploit Kit

- Tricks: You see two of the same files; the sizes are different, sometimes significantly
- Look at the file headers for that file type and compare. Using the LSB method, the human eye cannot see the differences in color.
- JPEG files start with FF D8 and end in FF D9
IOT’s Dark Passenger
31% of Victims Experienced DESTRUCTIVE ATTACKS
Cybercriminal Behavior has evolved
Kill Chains

Lockheed Martin KillChain 2011

MITRE ATT&CK 2018
Cognitive Attack Loop

1. RECON & INFILTRATE
2. MAINTAIN & MANIPULATE
3. EXECUTE & EXFILTRATE
Phase 1: Recon & Infiltrate

- Gather Intel
- Exploitation
- Social Engineering
- Delivery
Phase 2: Maintain & Manipulate

- Execute
- Privilege
- Persistence
- Evasion
- Communication
Phase 3: Execute & Exfiltrate

- Capture
- Exfiltrate
- Destruction
- Disinformation
Next-Generation Cybersecurity
Digital CCTV: Unfiltered Endpoint Data:

The best security data is continuous, unfiltered, and centralized endpoint data.

- **Continuous**: Full visibility into attacks
- **Unfiltered**: Detection & prevention of known and unknown attacks
- **Centralized storage**: Guaranteed availability for integrations and advanced analytics

1. Executions
2. Network Connections
3. File Modifications
4. Registry Modifications
5. Cross-process Events
6. Unique Binaries
CB UEX Community

92
Threat Intel
Notifications Posted

20,000 +
Community Members

425
Pieces of Community Based Threat Intel

Welcome to the Carbon Black User Exchange

Tap into the knowledge of thousands of security professionals around the globe

Search

The Carbon Black User Exchange has more than 20,000 security professionals who share best practices and threat intelligence to improve their security posture and help combat threats.

Latest Threats
View the latest threat research, or share new discoveries with the community

Follow Your Product Page
Find resources and join the latest discussions for your product

Get Help
Access self-service resources or contact our support team
Questions
@TAKellermann