Taste the Rainbow

Dave Hartley - MWR InfoSecurity

BSIDES NYC

MWR

GREETINGS' PROGRAMS!

- Director @mwrinfosecurity | @mwrlabs - UK.
- CHECK TL, CREST CC, CSAS & CSAM.
- 

- CBEST (UK), TBEST (UK), GBEST (UK), TIBER (NL) & ICAST (SG).

Agenda

- Rainbow Teaming
- Evolving TTP's
- Defenses

TEAM RAINBOW

MWR

Pink Team?

- **Black -** Physical
- **Red -** Digital Offensive
- **Blue -** Detection and Response
- **Purple -** Red & Blue working together
- **Gold -** Crisis Management

What is Rainbow Team(ing)?

- I've been around long enough to see the consulting industry come full circle.
- When I started we were invited to 'penetrate' a client and get as far as we could. Often the challenge was "put a file on my desktop" with 0 knowledge.
- It then became you can't do this, you can't do that, just do this, only do that. Tight and narrow scoped assessments of $thing in isolation.
- Now we're back to come at me bro.

What is Rainbow Team(ing)?

- Red Team means different things in UK vs US.
- PRA/FCA (BoE) have created a Red Team for compliance purposes.
- Power and Energy, Telco, Space, etc also.

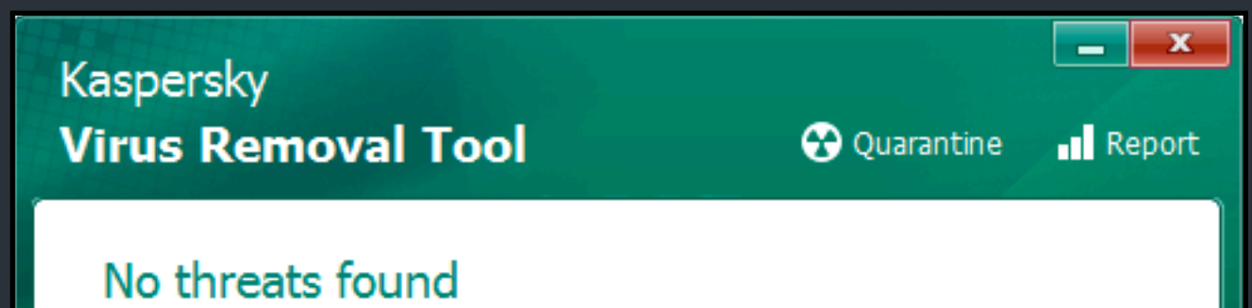
Full Spectrum Cyber

- Full Spectrum Cyber - Northrop Grumman.
- Full Spectrum Attack Simulation - NCC.
- Targeted Attack Simulation - MWR.
- Simulated Attack - CREST.
- Rainbow Team?

- It doesn't really matter what you call it - as long as it has value!
- Should be a custom solution built around objectives and have business impact.
- Not going to cover Black. Following is in order I would prioritize.

Blue

- Validate and verify your assumptions / confirm your existing investment - does what it says on the tin?
- Tune those detection sensors / boxen with blinkenlights.
- Att&ck - Caldera | MWR AttackSim | Roll Your Own
- Christopher Payne (Target) - Steel Sharpens Steel: Using Red Teams to improve Blue Teams.



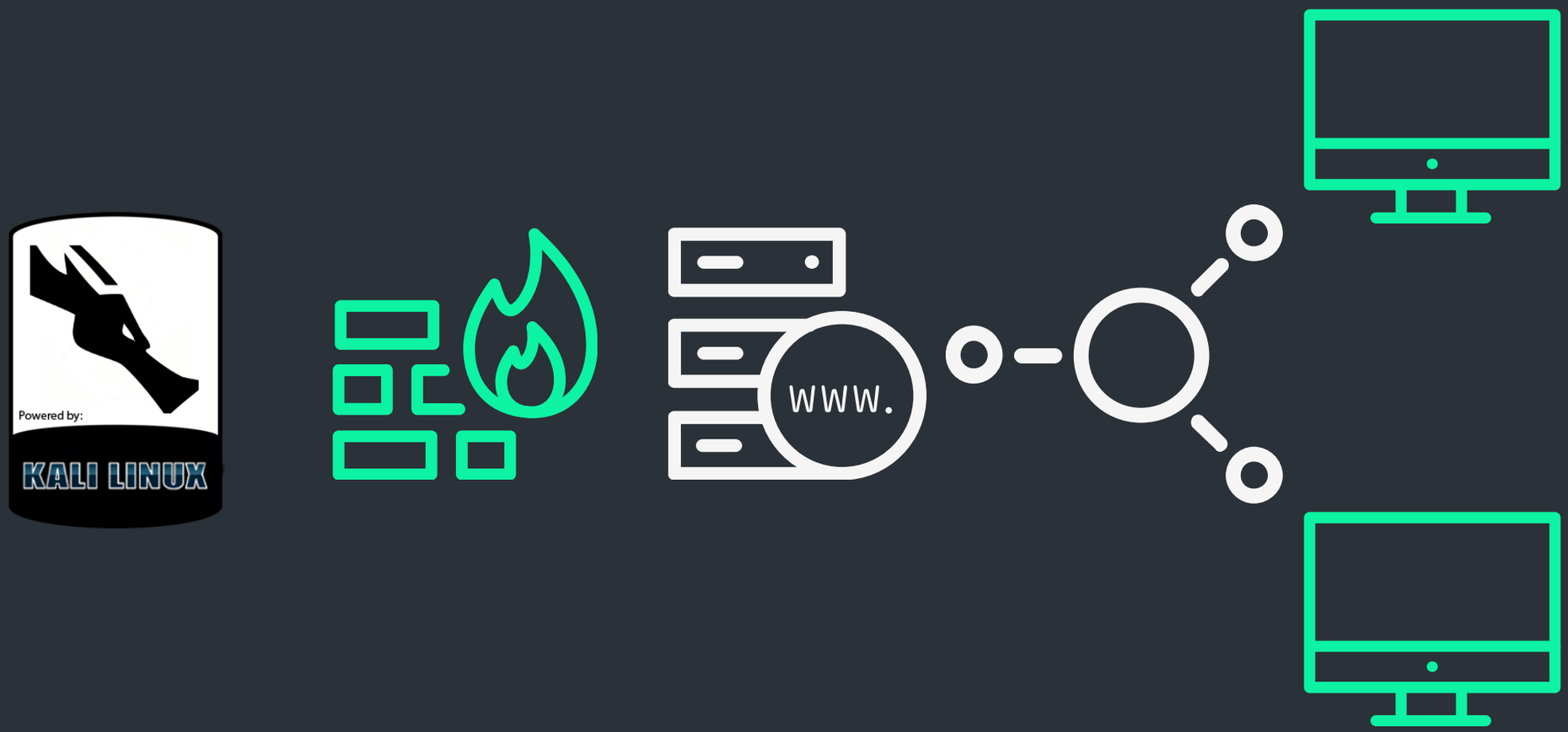
- Run a **Red** to put **Blue** through a live fire round.
- Get maximum value by including a **Purple** session and using the exercise as basis for a post op **Gold** workshop.

Evolving TTP's

Tactics, Techniques, and Procedures Guide

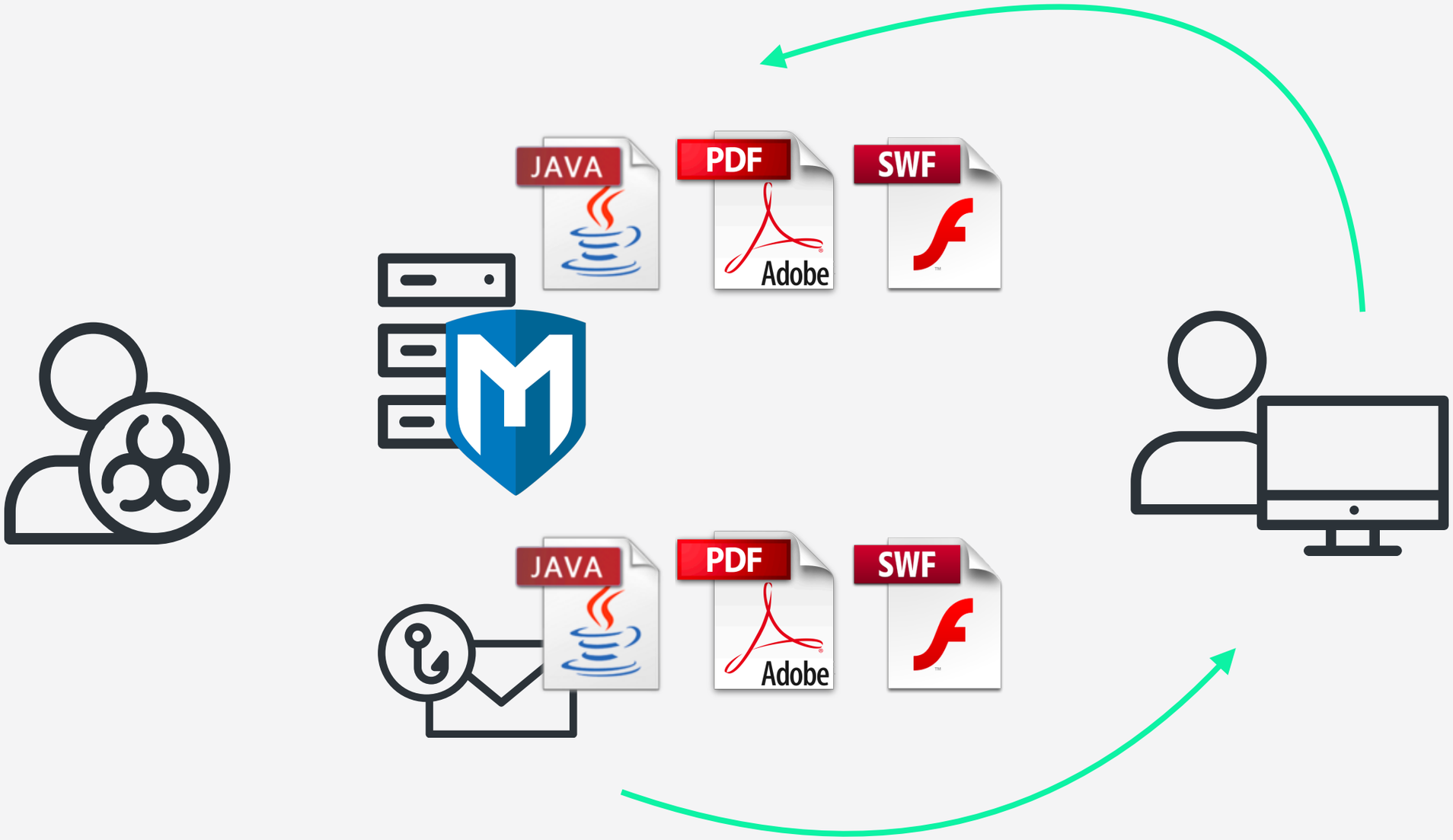
MWR

Good Old Days



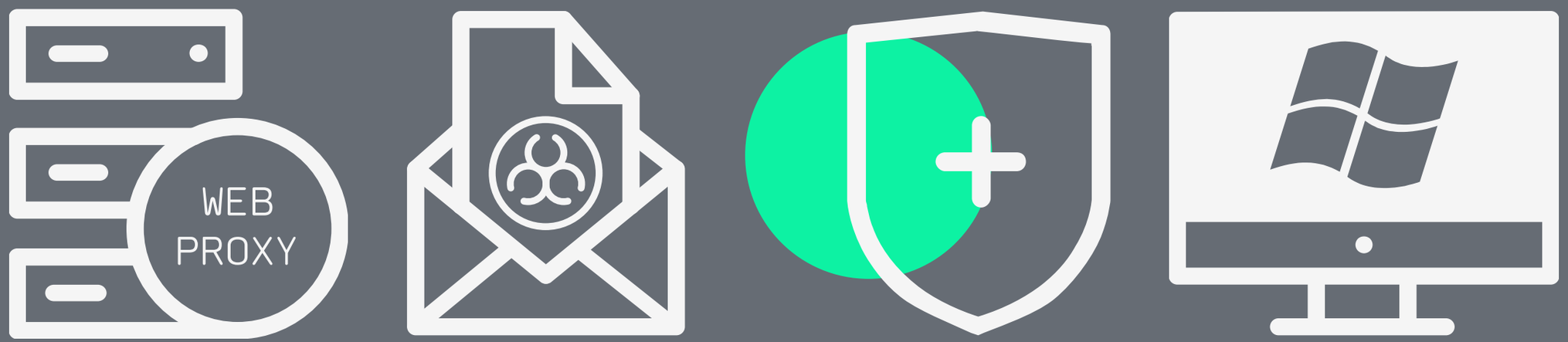
MWR LABS

Browsers & Extensions



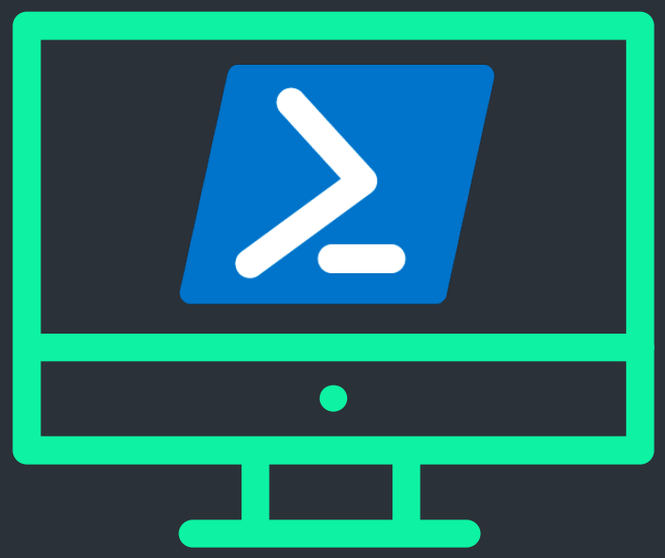
MWR LABS

Blinkenlights & Boxen



MWR LABS

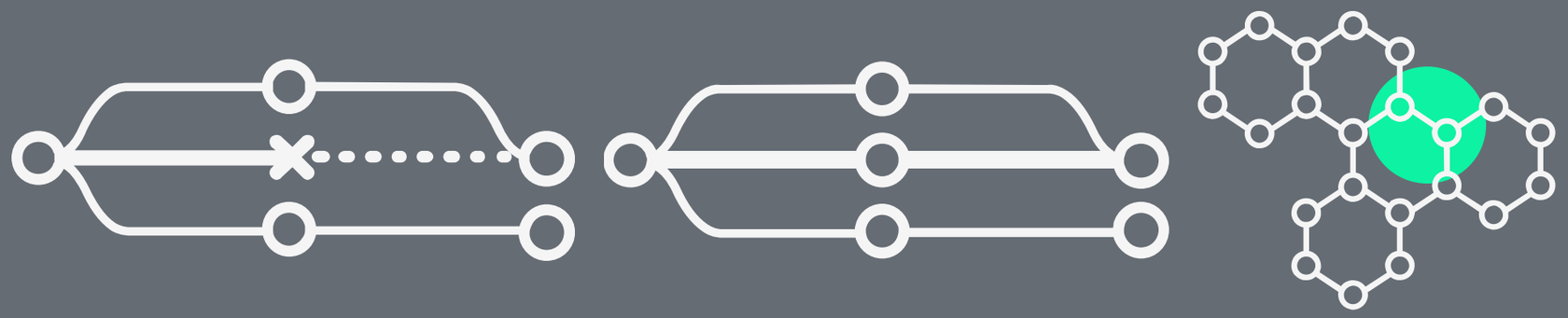
Back Orifice



MWR

MWR LABS

Post Compromise



- Cobalt Strike | Powershell Empire
- PowerUp | Kerberoasting
- SPN | Find-InterestingFile | AD Control Map (MWR Bloodhound)
- Credential theft shuffle PSexec | Mimikatz | Pass-The-Hash et al.

SPECTEROPS

Veris Group ATD Adaptive Threat Division

MWR

MWR LABS

EDR | ETDR | NGAV

CYLANCE

TANIUM™

CROWDSTRIKE

Microsoft ATA

cybereason

FireEye™

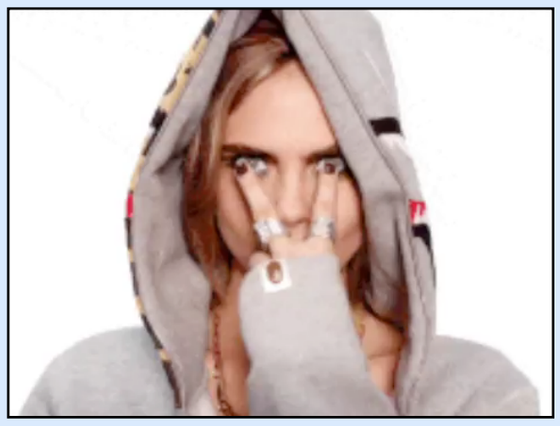
Symantec™

Carbon Black.

COUNTERCEPT

MWR

Spoilsports

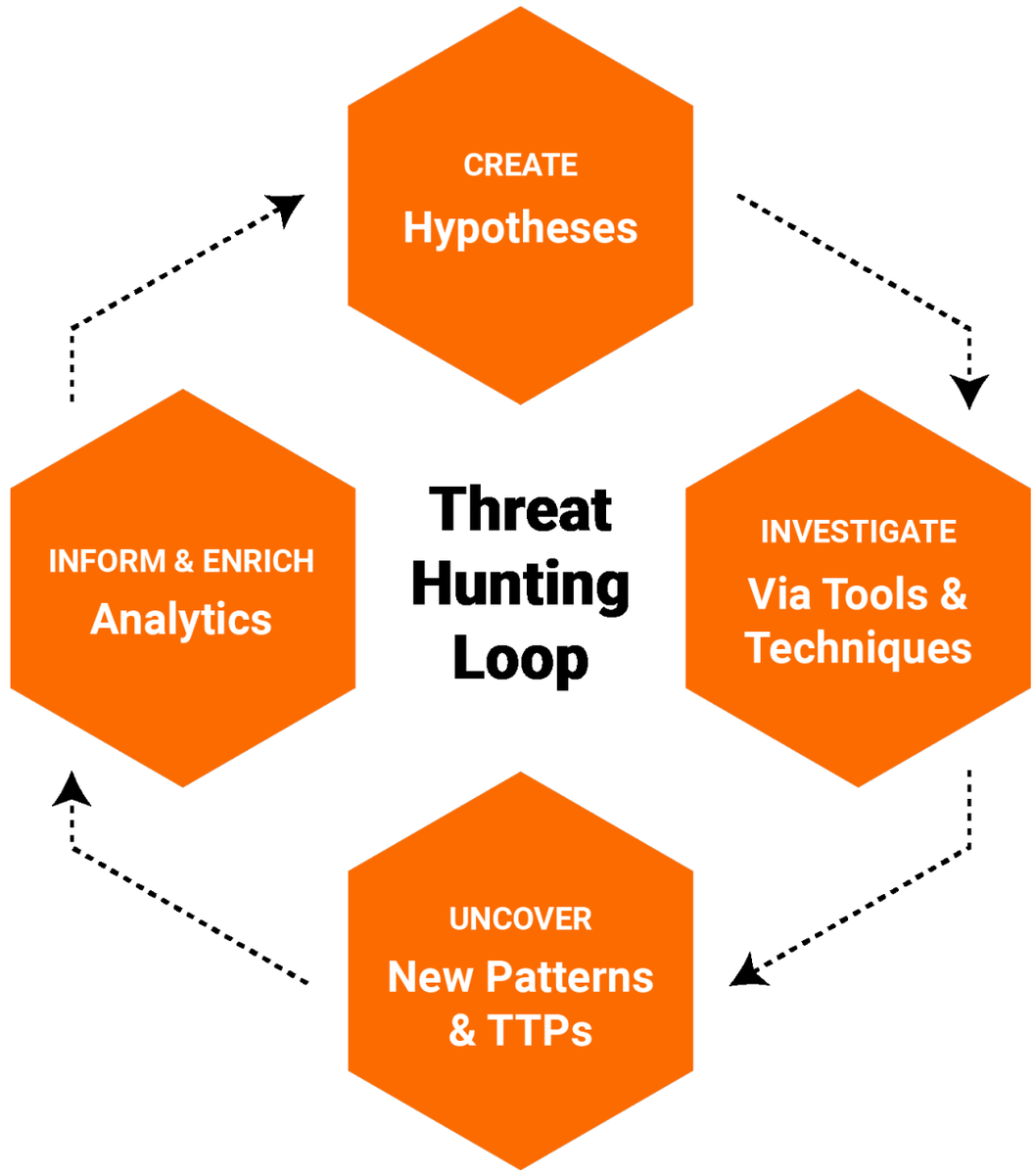


- PS - the ride is over. They're on to us. Logging, Constrained Language Mode, Just Enough Admin support.

- Macro (from untrusted) blocked, DDE Disabled, no more executable Outlook rules (HKCU key).

- App Locker / SRP / White Listing - people are starting to take this seriously.

Thrunters are Thrunting

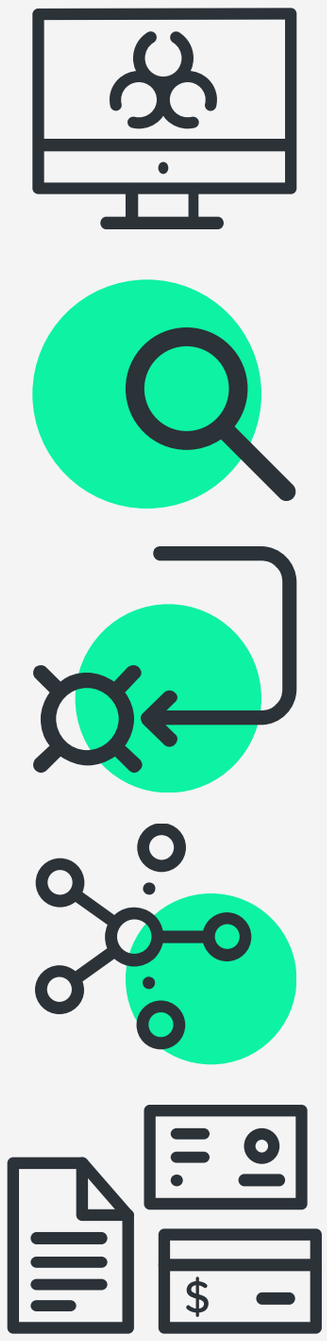


https://www.countercept.com/managed-threat-hunting

impervious

Get In & Get Out

- Get a foothold and persist.
- Gather some intel and do some recon.
- Move laterally and persist.
- Execute.
- Get out alive.



FROM RUSSIA WITH LOVE

John Lambert

@JohnLaTwC

General Manager, Microsoft Threat Intelligence Center,
johnla(AT)microsoft.com,
linkedin.com/in/johnjlambert

Payloads

- Avoid attachments, if you can. Usually less controls on web downloads, not often sandboxed.

- Client side script JS / VBS (avoid Kernel32 API calls) - e.g. CACTUSTORCH from MDSEC and SharpShooter (includes sandbox evasion); both leverage DotNet2Jscript from James Forshaw.

- Stageless custom executables that also leverage COM / DLL hijacking techniques.

- Take heed of DLL / memory injection / process hallowing, look to Doppelgänging also? See CS OpSec blog.

MWR - **Inappropriate Touch** (custom implant - in Dev).

MWR LABS

';--have i been pwned?

Office 365

yammer

MWR LABS

COMING SOON!

Custom Command & Control (C3)

Dropbox

Google Drive

OneDrive

Office 365

IMAP

SMB

COBALT STRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS

MWR

Don’t get Burned

- Post exploitation avoid PS and stay away from system.management.automation (InsecurePowerShell?).

- Recon via limited SPN / Kerberoasting. Live off The Land and use WMI, LDAP, biz tools like SCCM (hunt with it too), Intranet (SharePoint, Confluence, Wiki). Stay away from DCs.

- Lateral Movement via Trojan files, RDP, SCCM / Altiris, GPO Tasks - try not to leave a straight line / trail. Use tickets if you can (Silver). Use AES for Over-PTH, Golden Tickets.

Know your Enemy

- Turn your targets defenses against them and/or operate within them.
- Smash and Grab (MTTD).
- Deception.
- Diversions.

MWR LABS

Defense

Defense

- E-Mail gateway security solution block attachments from untrusted sources, sandbox all incoming, crawl to site and do same (also SPF, DKIM and DMARC).

- 2FA on all external services (including 3rd party cloud).

- Web proxy and only resolve internal DNS internally.

- Isolate workstations and restrict to their BizOps servers and services (segment critical systems). Operate least privilege for all.

- Red Forest (ESAE) - LAPS, PAW & PAM, JEA & JIT?

Defense: endpoint

- Run latest and greatest everything.
- Whitelist / App Locker / SRP etc. disable and/or remove / Macro, VBA, PowerShell, JScript, VBScript - all the things.
- Deploy AV, NGAV, EDR, ETDR - stick it all on.

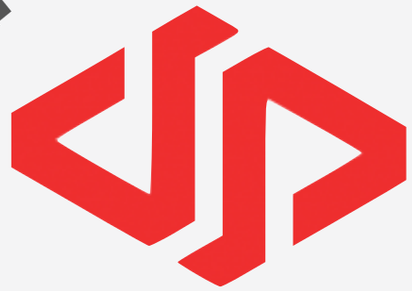
Defense: people

- Benchmark, invest and train Blue Team.
- Educate, enable, support and enlist users (DevSecOps philosophy). Give them a channel to raise alarms / come and speak to SecOps etc.
- Keep Blue Team match fit with regular Red Team sparring matches (Purple philosophy).

Good People & Tool Smiths

- Dominic Chell and Vincent Yiu (MDSec) - A Year In The Red.
- Christopher Payne (Target) - Steel Sharpens Steel: Using Red Teams to improve Blue Teams.
- @malwareunicorn - .NET Hijacking to Defend PowerShell (presentation and paper).
- @retBandit (IBM) - Red Team Techniques for Evading, Bypassing & Disabling Advanced Threat Protection and Advanced Threat Analytics.






MWR LABS

The End

@mwrlabs | @mwrinfosecurity | @countercept

MWR

FAQ

- I only have budget for **Red**, **Blue**, **Purple** or **Gold** - which one do I do first?
- Investing in people is expensive, how do I get budget / buy in?
- I spent a fortune on $tech, is it worthless / what $tech is best?

Offensive Tooling

- PEAS is a tool for running commands on an ActiveSync server e.g. Microsoft Exchange - https://github.com/mwrlabs/peas.

- WePWNise generates architecture independent VBA code to be used in Office documents that automagically bypasses application controls and exploit mitigations - https://github.com/mwrlabs/wePWNise.

- C3 uses Cobalt Strike External C2 feature to implement beacon compatible esoteric C2 channels.

- XRulez is a tool for creating malicious outlook rules - https://github.com/mwrlabs/XRulez for persistence purposes.

Light Reading

- Recon - https://labs.mwrinfosecurity.com/blog/active-directory-users-in-nested-groups-reconnaissance, https://labs.mwrinfosecurity.com/blog/visualising-organisational-charts-from-active-directory & https://labs.mwrinfosecurity.com/blog/offline-querying-of-active-directory.

- Code execution (avoiding command line logging) using COM objects from within VBA or DLL (whitelist bypass) - https://labs.mwrinfosecurity.com/blog/dll-tricks-with-vba-to-improve-offensive-macro-capability

- Safer Implants: https://labs.mwrinfosecurity.com/blog/safer-shellcode-implants & Hiding Implants in plain sight - https://labs.mwrinfosecurity.com/blog/masquerading-as-a-windows-system-binary-using-digital-signatures.

- Office Persistence - https://labs.mwrinfosecurity.com/publications/one-template-to-rule-em-all & https://labs.mwrinfosecurity.com/blog/add-in-opportunities-for-office-persistence.

- Lateral Movement - https://labs.mwrinfosecurity.com/blog/abusing-putty-and-pageant-through-native-functionality & https://labs.mwrinfosecurity.com/blog/trust-years-to-earn-seconds-to-break.

BSIDES NYC