ACCESS42

HANDLING THE MODERN-DAY ATTACKER WITH A DEFENSIVE LAYERED APPROACH (SOC)

Stefan Lambregts

CCV CYBER PENTEST

Digitrust NEN 7510

Digitrust ISO 27001

ACCESS42 Cybersecurity

Stefan Lambregts

Manager Operations

AGENDA

The Modern-Day attacker

The attack path

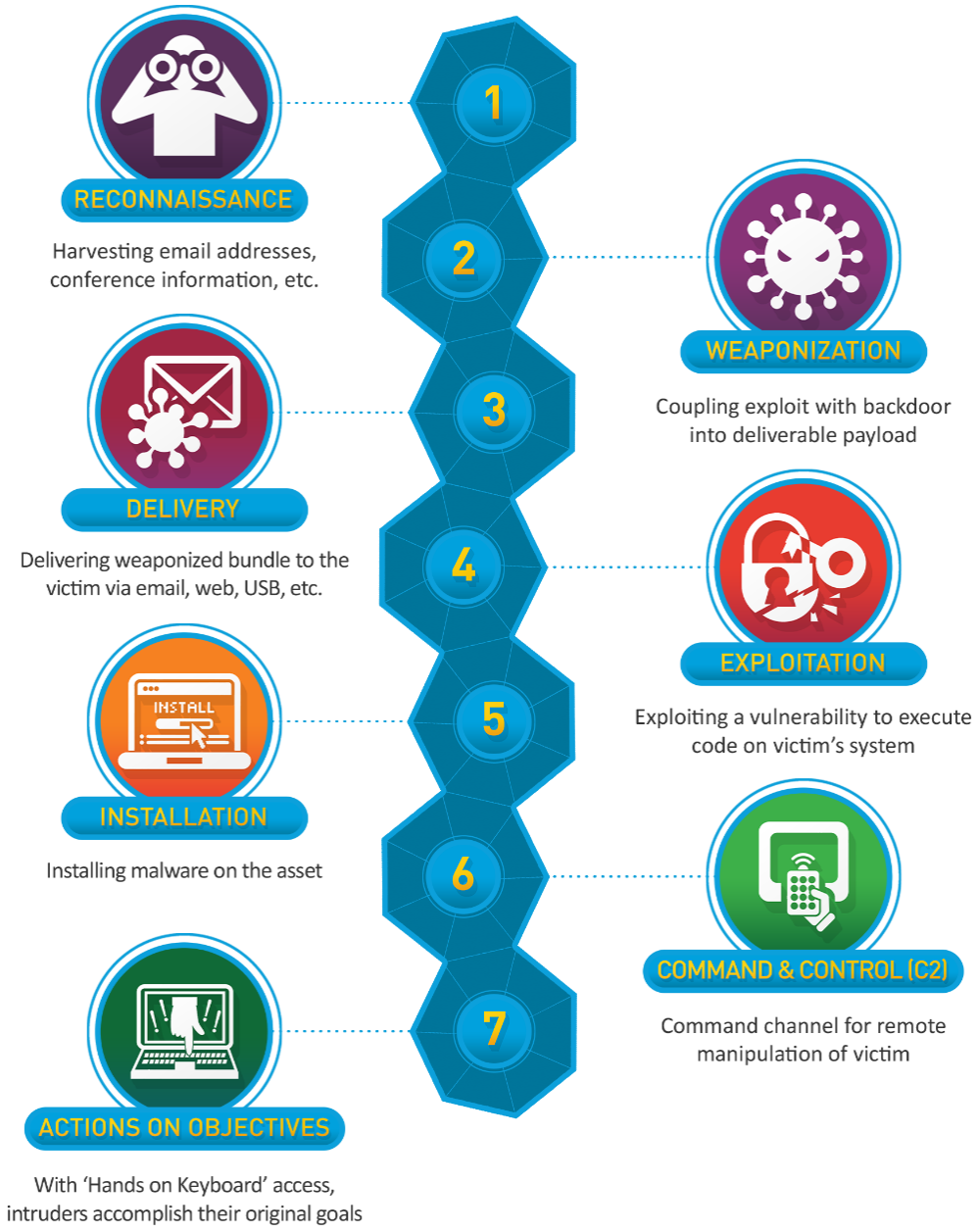
Layered defense

Correlation

"TODAY'S ATTACKERS DON'T JUST HACK—THEY LOG IN, THEY WAIT, THEY BLEND IN."

ACCESS42
Cybersecurity


This is Alex. He is a **skilled**, **patient** and **opportunistic** hacker



RECONNAISSANCE

Firstname.Lastname@innotech.com

InnoTech

WEAPONIZATION + DELIVERY

hr-portal@update.innotech-benefits.com Tuesday, April 15, 20

❗ Mandatory Action: 2025 Benefits Package Update

Hi Karen, InnoTech_Benefits_Update_202

As part of our annual compliance and benefits review, we're roiling out the updated InnoTech 2025 Employee Benefits Package.

To ensure continued access to your benefits, please download and review attached Benefits Summary & Acknowledgment Form:

InnoTech_Benefits_Update_2025.xlsm *(Macro-enabled file* – required for digital signature validation)
https://update.innotech-benefits.com/files/Benefits_Update_2025.xlsm

Thank you for your prompt attention to this matter.

Warm regards,
Angela Morris
Senior HR Specialist
InnoTech Corporation

This is Karen. She is a **non-technical, unsuspecting** and **overprivileged** HR employee.

EXPLOITATION

Microsoft Office Remote Code Execution Vulnerability

CVE-2024-30101

Security Vulnerability

Released: Jun 11, 2024

INSTALLATION

COMMAND & CONTROL

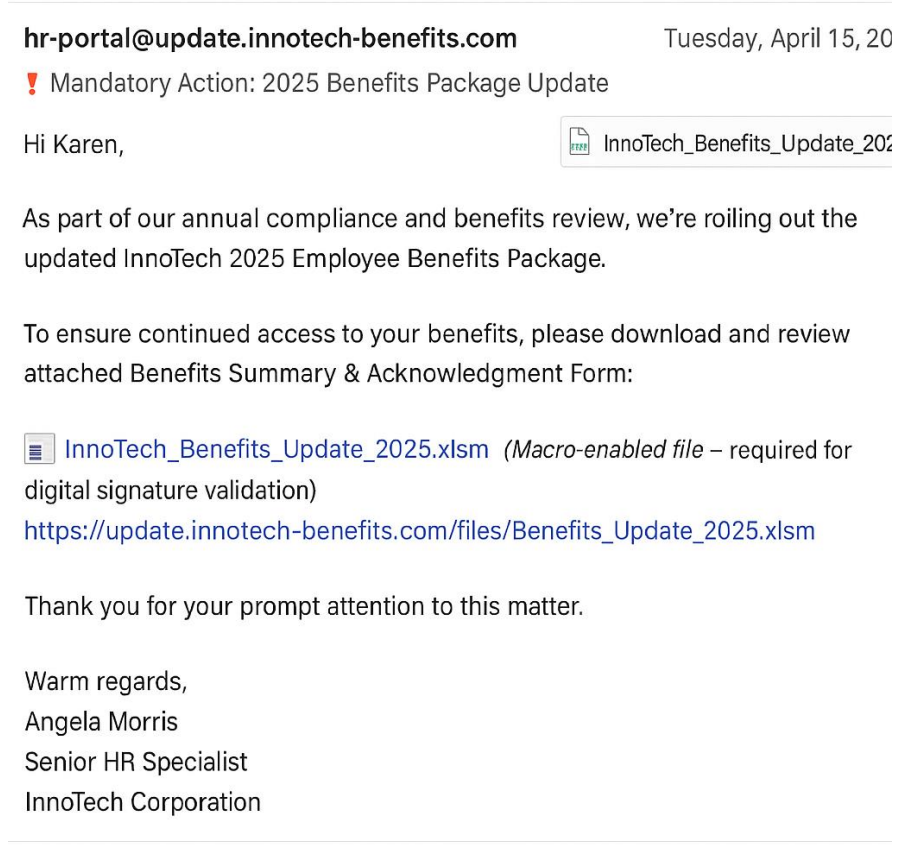
ACTIONS ON OBJECTIVE


“Ransomware isn’t just a last-stage problem—it’s the **result** of missed detections at earlier stages. By building layered defenses and correlating events across phases, we can stop attackers like Alex before they do damage.”

WEAPONIZATION + DELIVERY

Email Security

- Anti-Spoofing
- Detects malicious attachments & links
- Human risk



hr-portal@update.innotech-benefits.com Tuesday, April 15, 20

❗ Mandatory Action: 2025 Benefits Package Update

Hi Karen,

InnoTech_Benefits_Update_202

As part of our annual compliance and benefits review, we're roiling out the updated InnoTech 2025 Employee Benefits Package.

To ensure continued access to your benefits, please download and review attached Benefits Summary & Acknowledgment Form:

InnoTech_Benefits_Update_2025.xlsm *(Macro-enabled file* – required for digital signature validation)
https://update.innotech-benefits.com/files/Benefits_Update_2025.xlsm

Thank you for your prompt attention to this matter.

Warm regards,
Angela Morris
Senior HR Specialist
InnoTech Corporation

ACCESS42 Cybersecurity

EXPLOITATION

Vulnerability Management

- Reduce risk of exploitation
- Prioritize based on risk

Microsoft Office Remote Code Execution Vulnerability

CVE-2024-30101
Security Vulnerability

Released: Jun 11, 2024

INSTALLATION

Endpoint Detection & Response

- Real-Time threat detection
- Enhanced endpoint protection
- Rapid response & containment

COMMAND & CONTROL

Cloud Infrastructure Entitlement Management

- Least privilege enforcement
- Visibility into cloud permissions

ACTIONS ON OBJECTIVE

Network Detection & Response

- Deep visibility into network traffic
- Detect lateral movement

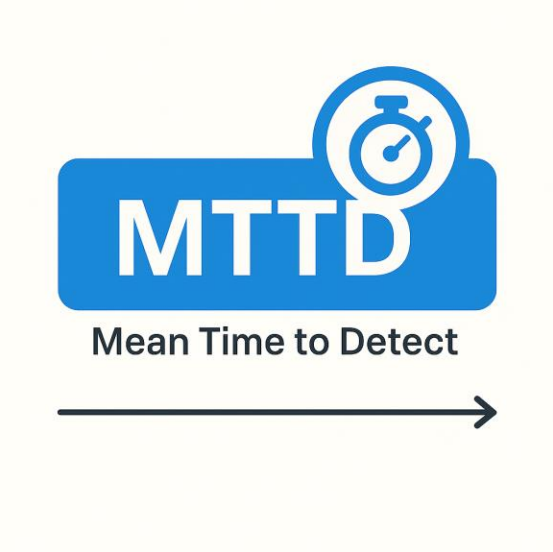
"IT'S NOT ABOUT HAVING MORE TOOLS—IT'S ABOUT MAKING THE TOOLS WORK TOGETHER."

ACCESS42 Cybersecurity

SECURITY OPERATIONS CENTER

- Single pane of glass
- Rapid detection & response
- Defense in depth enforcement
- Correlation is key

CORRELATION IS KEY



"The faster you see it, the faster you stop it."

CORRELATION

Phishing detection + Endpoint behavior

Scenario: Karen opens the phishing email and downloads the malicious Excel file

- Email Protection: Flags email as suspicious due to spoofed sender domain or anomalous attachment
- EDR: Detects macro-enabled Excel spawning PowerShell or abnormal child processes

Correlation via SIEM/XDR: A rule correlates a phishing alert with suspicious endpoint behavior (Office app executing PowerShell) within the same user session

Prevention/Alert Outcome: Automatically quarantines the endpoint for investigation. Could prevent payload execution entirely.

CORRELATION

EDR + Identity Behavior

Scenario: Alex used Mimikatz to dump cached credentials from the memory of Karens device

- EDR: detects an untrusted process
- Identity Provider: Karen's account is suddenly logged in as Domain Admin

Correlation via SIEM/XDR: Privilege escalation immediately after credential dumping

Prevention: Lock account, revoke token & isolate system

THANK YOU

Stefan Lambregts

stefan@access42.nl

www.access42.nl