USB Drive-by

An employee picked up a worm on their work machine after plugging their USB device into a communal computer at a print shop, giving the attackers access to the internal network.

DETECTION

Endpoint Analysis
Endpoint Security Protection Analysis

TOOLS

USB Rubber Ducky
Bash Bunny

https://redcanary.com/blog/raspberry-robin/

https://attack.mitre.org/techniques/T1091/

RED CANARY

Compiled After Delivery

The attackers assembled their files on an endpoint by delivering text-based source code and using that compromised system's native compiler.

DETECTION

Endpoint Analysis
Endpoint Security Protection Analysis

TOOLS

GCC
csc.exe
Atomic Red Team™

https://attack.mitre.org/techniques/T1027/004/

RED CANARY

Gatekeeper Bypass

The attackers bypassed Apple's Gatekeeper functionality and tricked a user into downloading a malicious file on a macOS endpoint.

DETECTION

Endpoint Analysis
Endpoint Security Protection Analysis
Network Threat Hunting - Zeek/RITA Analysis

TOOLS

certutil
codesign
Atomic Red Team™

https://attack.mitre.org/techniques/T1553/001/

RED CANARY

Obfuscated Payload Delivery

The attackers installed a malicious executable that evaded signature-based analysis by encoding and splitting its payload.

DETECTION

Endpoint Analysis
Endpoint Security Protection Analysis
Memory Analysis

TOOLS

ADVobfuscator
Manual fuzzing/string splitting
Base64 encoding

https://attack.mitre.org/techniques/T1027/

RED CANARY

RFID Theft

The attackers used a Flipper Zero to copy the Radio Frequency Identification (RFID) signal from an IT employee's entry badge and gained physical access to the server room.

DETECTION

Physical Security Review
User and Entity Behavior Analytics (UEBA)

TOOLS

Flipper Zero

https://docs.flipperzero.one/

Disabling Windows Defender

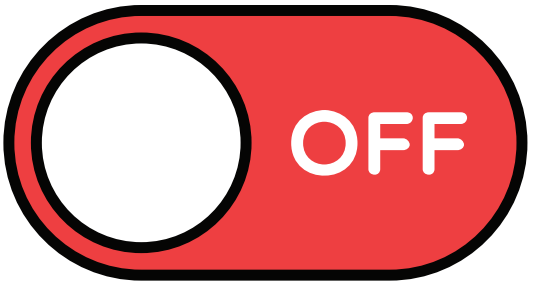
The attackers use PowerShell commands and scripts to disable Windows Defender, enabling them to bypass file inspection controls designed to prevent malware.

DETECTION

Endpoint Analysis
Endpoint Security Protection Analysis
SIEM Log Analysis

TOOLS

Cobalt Strike
BloodHound
Atomic Red Team™



https://attack.mitre.org/techniques/T1059/001/

RED CANARY

Process Injection

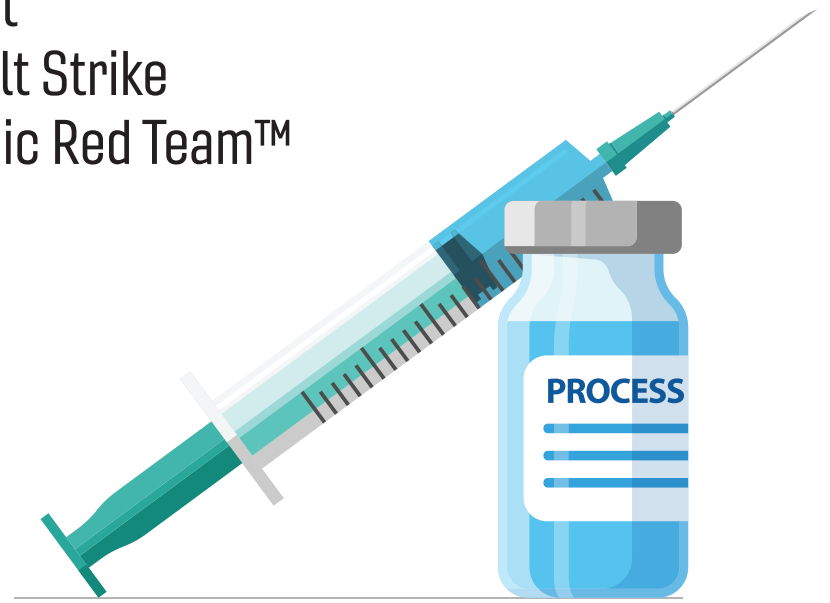
The attackers inject their payload into a legitimate, privileged process.

DETECTION

Endpoint Analysis
Endpoint Security Protection Analysis
Memory Analysis

TOOLS

Donut
Cobalt Strike
Atomic Red Team™



https://attack.mitre.org/techniques/T1055/

RED CANARY

LSASS Credential Dump

The attackers dump the contents of the Local Security Authority Subsystem Service (LSASS) process memory, gaining access to legitimate account credentials.

DETECTION

Endpoint Analysis
Endpoint Security Protection Analysis
Memory Analysis
User and Entity Behavior Analytics (UEBA)

TOOLS

Mimikatz
ProcDump
comsvcs.dll
Atomic Red Team™

https://attack.mitre.org/techniques/T1003/001/

RED CANARY

Application Control Bypass

The attackers use Rundll32 to execute malicious code while avoiding detection.

DETECTION

Endpoint Analysis
Endpoint Security Protection Analysis

TOOLS

Cobalt Strike
Metasploit
Rundll32
Atomic Red Team™

RUNDLL32

https://attack.mitre.org/techniques/T1218/011/

RED CANARY

Read/Write With chmod 777

The attackers turn their attention to your *nix machines and want all the permissions! They're using misconfigured user and group permissions to run in a different user's context.

DETECTION

Endpoint Analysis
Endpoint Security Protection Analysis
User and Entity Behavior Analytics (UEBA)
Cyber Deception

TOOLS

find
chmod
Atomic Red Team™

https://attack.mitre.org/techniques/T1548/001/

RED CANARY

PsExec Abuse

The attackers use PsExec to move laterally and gain control of additional systems.

DETECTION

Endpoint Analysis
Endpoint Security Protection Analysis
Network Threat Hunting - Zeek/RITA Analysis
SIEM Log Analysis

TOOLS

Net
PsExec
Atomic Red Team™
A fax machine

https://attack.mitre.org/techniques/T1021/002/

RED CANARY

Lateral Tool Transfer

The attackers move a malicious payload from a system they initially compromised to a new host on the same network.

DETECTION

Endpoint Analysis
Endpoint Security Protection Analysis
Network Threat Hunting - Zeek/RITA Analysis
SIEM Log Analysis

TOOLS

PsExec
PowerShell
Cobalt Strike
BITSAdmin

FREE DELIVERY

https://attack.mitre.org/techniques/T1570/

RED CANARY

Authorized Remote Tools

The attackers use an authorized remote administration tool to exfiltrate confidential information.

DETECTION

Endpoint Analysis
Network Threat Hunting - Zeek/RITA Analysis
User and Entity Behavior Analytics (UEBA)

TOOLS

ScreenConnect
rsync
NetSupport
AnyDesk

https://attack.mitre.org/techniques/T1219/

RED CANARY

Cloud Services as Exfil

The attackers hitch a ride on the application access tokens for your cloud-based resources. It's a good thing they didn't crash your Kubernetes, but not all is well; they leverage your API to exfiltrate data.

DETECTION

User and Entity Behavior Analytics (UEBA)
Server Analysis
Cyber Deception

TOOLS

AADInternals
Peirates

https://attack.mitre.org/techniques/T1528/

RED CANARY

Bluetooth as Exfil

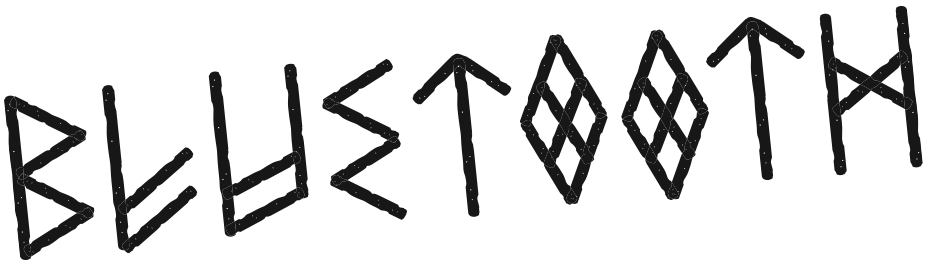
The attackers knew you were watching that wired connection closely and got crafty—they exfiltrate all that valuable data via a Bluetooth-enabled device.

DETECTION

Endpoint Analysis
Physical Security Review

TOOLS

Blue Pigeon



https://attack.mitre.org/techniques/T1011/001/

RED CANARY

Malicious Access Point

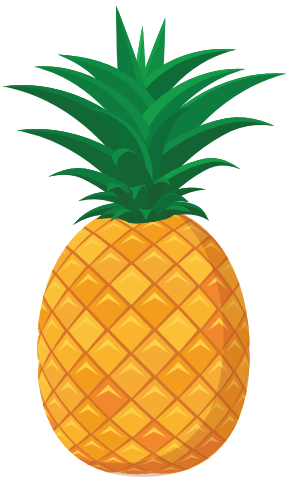
The attackers hide an access point spoofing a legitimate ESSID in a plant pot in the lobby! Unsuspecting employee devices connect to it when they're nearby. This is a Machine-in-the-Middle (MitM) strategy.

DETECTION

Endpoint Analysis
Endpoint Security Protection Analysis
Network Threat Hunting - Zeek/RITA Analysis
Physical Security Review

TOOLS

WiFi Pineapple®



RED CANARY

Event-Triggered Execution

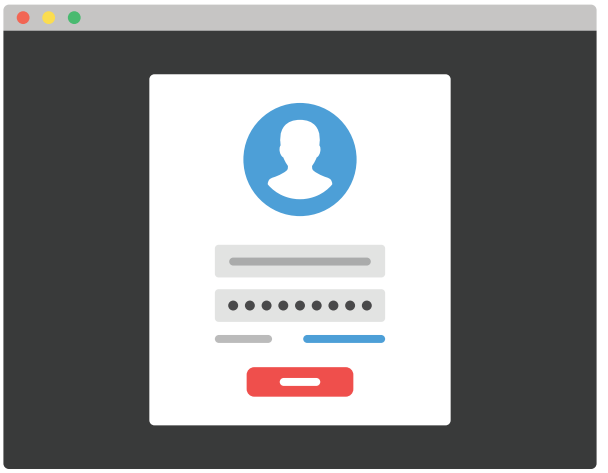
The attackers use a permanent WMI event subscription to execute a malicious payload anytime the user logs in.

DETECTION

Endpoint Analysis
Endpoint Security Protection Analysis
Server Analysis

TOOLS

Cobalt Strike
Atomic Red Team™



https://attack.mitre.org/techniques/T1047/

RED CANARY

Scheduled Task

The attackers have made themselves immortal by using a scheduled task on a Windows system to persistently run malicious code every 30 minutes.

DETECTION

Endpoint Analysis
Endpoint Security Protection Analysis
SIEM Log Analysis

TOOLS

Koadic
NetWire
Atomic Red Team™

https://attack.mitre.org/techniques/T1053/005/

RED CANARY

Rename Process

The attackers change the name of a system utility to make their malicious executions look benign.

DETECTION

Endpoint Analysis
Endpoint Security Protection Analysis
Memory Analysis

TOOLS

Rundll32
Atomic Red Team™

https://attack.mitre.org/techniques/T1036/003/

RED CANARY

Spawn Web Shell

The attackers abuse the Internet Information Services (IIS) worker process to install a web shell on a Windows web server.

DETECTION

Endpoint Analysis
Endpoint Security Protection Analysis
Server Analysis
Network Threat Hunting - Zeek/RITA Analysis

TOOLS

Cobalt Strike
Empire
NetWire
Atomic Red Team™

https://attack.mitre.org/techniques/T1059/003/

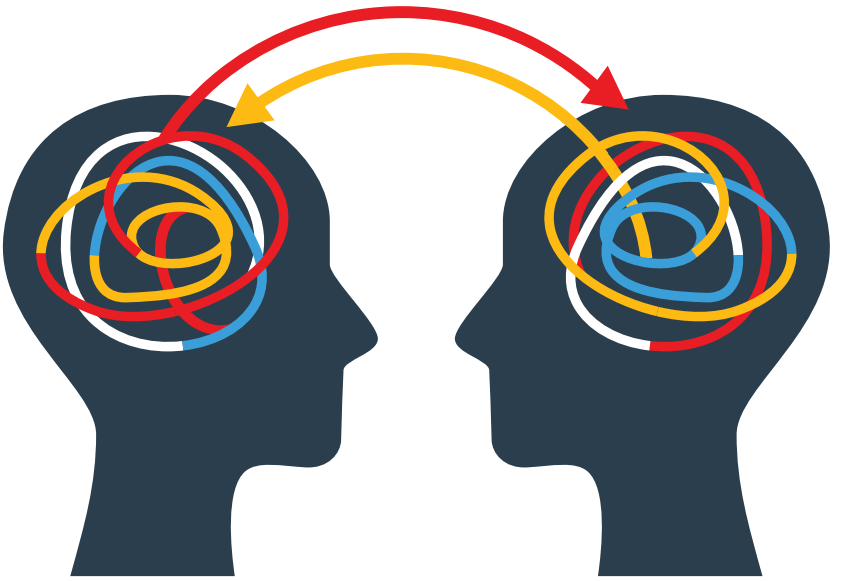
RED CANARY

Call a Consultant

Do you want help? Feeling stuck? Rolling badly? Need a different perspective on the incident? Then maybe it's time to phone a friend.

You can choose one Consultant Card to help your team with the incident.

The Consultant Card's modifier is effective immediately.



RED CANARY

Physical Security Review

Do you have security cameras? Do you have security guards? Do you have access badges for certain areas in your facilities? Can just anyone access your sensitive IT infrastructure? No? Are you sure?

RED CANARY

Missed Payday

The attackers compromise your email account, email HR, and instruct them to update your direct deposit information, routing your paycheck into a bank account they control.

NOTES

Each of the Defenders must roll a D20 and the person with the lowest number has to get a night job as a bartender and must remain silent for the rest of the session.

RED CANARY

Not a Red Team

The network threat-hunting team has detected C2 beacons on multiple machines in your environment. The attackers can now install additional payloads on the affected machines.

NOTES

Have the Incident Captain draw an additional **Persistence** Card as well as a **Pivot and Escalate** Card.

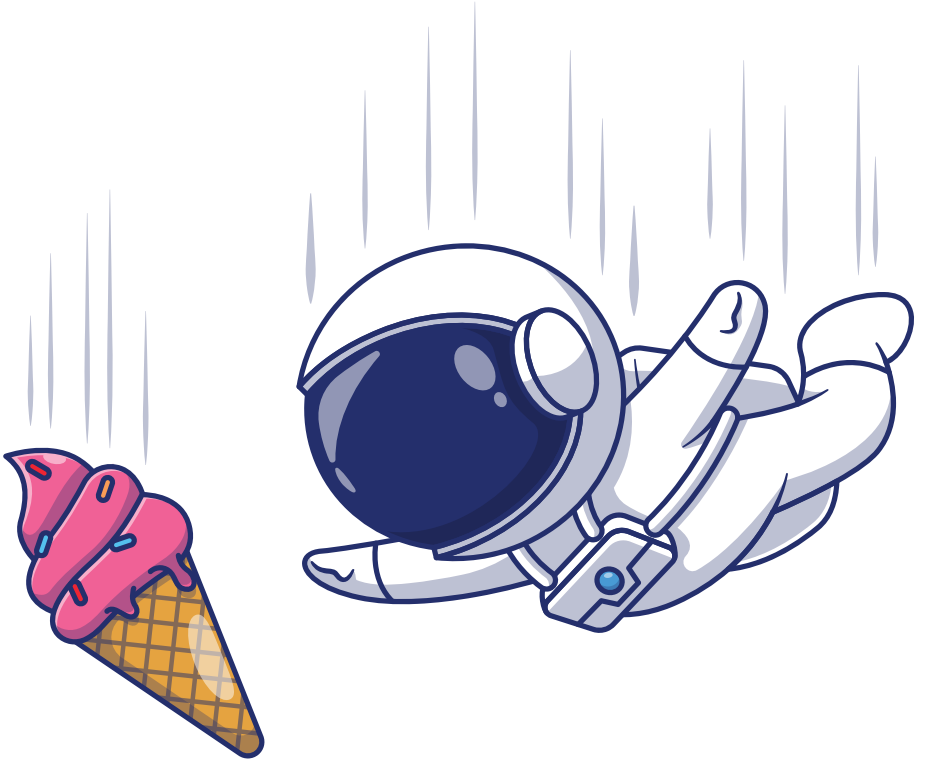
RED CANARY

Deez Registry Keyz Plz?

A wild malicious registry key appears. The bad news: It is on 50 endpoints that are now rampant with malware. The good news: Management cares.

NOTES

The Defenders get **3 additional turns** to help solve the incident and a **Consultant Card** of their choice without rolling a D20.



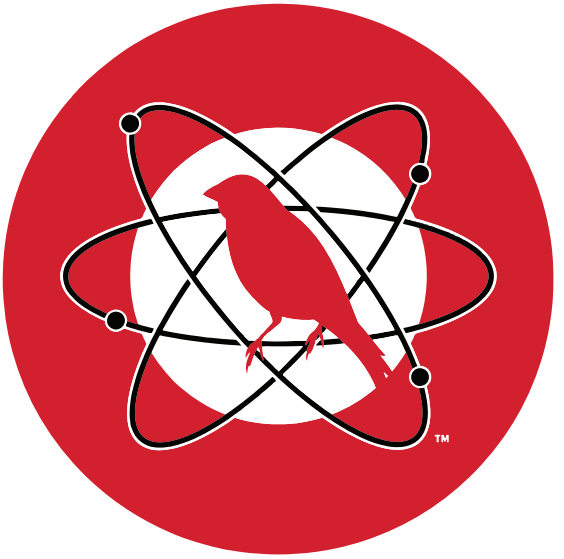
RED CANARY

Nuclear Test Site

Thank goodness the Defenders are Atomic Red Team™ power users and they are prepared for all the endpoint threats.

NOTES

The Defenders receive a **+2 modifier** on **Endpoint Analysis** and **Endpoint Security Protection Analysis** for the rest of the session.



https://atomicredteam.io/

RED CANARY

QUISHING

The local burger joint uses a QR code for its menu. How convenient! Unfortunately, a disgruntled ex-analyst knows the Defenders are regulars and put a malicious QR code over the legitimate one. Anyone who scanned it compromised their MFA device, which now needs to be wiped or replaced.

NOTES

The **Endpoint Security Protection Analysis** card is **unavailable** for the next **two turns**.

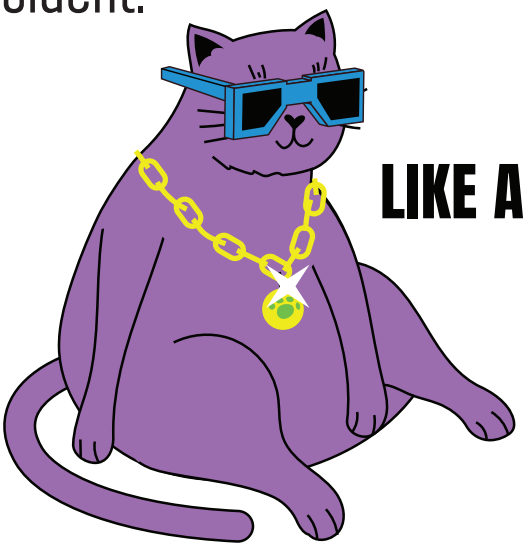
RED CANARY

Cat on Keyboard Deletes Production Database

Curiosity killed the database entries! A work-from-home administrator left their computer unlocked and, in an attempt to gain additional snuggles, their cat happened to spam out a mass delete on their keyboard. Oops.

NOTES

Each of the Defenders must roll a D20. The first two people to roll an odd number have to go fix the database and must remain silent for the rest of the session. Even number rollers move on to finish the incident.



RED CANARY

Undocumented System

That asset management and discovery project probably shouldn't have been put on hold. An undocumented system was just found on the enterprise domain and we don't really know anything about it. Who knows when this thing was spun up and for what?

NOTES

The machine had 200 Bitcoin from 2010. The Defenders order pizza and discuss if they're going to tell management or not.

RED CANARY

SNEAKY SNEAKY RAT

The attackers gain a foothold in the environment via remote access trojan (RAT). Now they're using it to load in external files and tools to further their reach. If this isn't under control soon, you'll have more than just RATs to worry about.

NOTES

Have the Incident Captain pull another set of **Attack Cards**. The Defenders get **five extra turns**.

https://attack.mitre.org/techniques/T1105/

RED CANARY

Adam Mashinchi

The Incident Captain must reveal the C2 and Exfil Card

SPECIALTIES

Product Management
Colorful but Dubious Metaphors
Command and Control Frameworks
Sketchy Scripts and Silly Websites
Open Source Security Tools
Privacy and Encryption

"Keep in mind that for the adversary, tactics, techniques, and procedures (TTPs) are side effects, not the intent."
- Adam Mashinchi

@Adam_Mashinchi
@Adam_Mashinchi @infosec.exchange

RED CANARY

Carrie Roberts

The Incident Captain must reveal all cards that list Atomic Red Team™ as a tool

SPECIALTIES

Red Teaming
Security Operations
Adversary Emulation
Training

"Prevention is ideal, but detection is a must."
Anonymous

@OrOneEqualsOne

RED CANARY

Mike Haag

The Incident Captain must reveal all cards that list SIEM as a detection source

SPECIALTIES

Threat Hunting
Atomic Testing
Threat Research
Detection and Response
Meme Connoisseur

"I am everywhere and nowhere."
- The Haag

@M_haggis

RED CANARY

RED CANARY MDR

Managed detection and response to secure your users, cloud, and endpoints.

We find the threats your security tools miss.

REDCANARY.COM

THREAT DETECTION REPORT

TECHNIQUES, TRENDS, AND TAKEAWAYS

Explore the most prevalent and impactful **threats**, **techniques**, and **trends** that we've observed in our annual retrospective.

REDCANARY.COM/TDR

RED CANARY READINESS EXERCISES

Continuously prepare for incidents with training, tabletops, and atomic tests in one engaging experience.

REDCANARY.COM/CYBERSECURITY-READINESS

ATOMIC RED TEAM™

An open source library of tests mapped to **MITRE ATT&CK™**, demystifying adversary tradecraft, and enabling security teams everywhere to test their defenses.

Contribute to the project

Join the Slack community

Subscribe to the Atomic Newsletter

ATOMICREDTEAM.IO

0010101101010101010

Backdoors™ & Breaches

For directions, visual guides, "how-to" videos, educational infosec resources, links to open-source virtual solutions, and to order additional core and expansion decks, visit:

www.backdoorsandbreaches.com