



Initial Access Tactics in Modern Malware

Pedro Urbina
Certified Ethical Hacker, Security+



Mitre ATT&CK Framework



Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

Exfiltration

Command & Control

Drive-By Compromise

Websites run scripts in the browser automatically all the time, malicious websites leverage this functionality to gain access to a user's system.

Legitimate websites can also be leveraged.

- Serving malicious ads via trusted ad providers
- Injected (XSS) payloads targeting all visitors
- Abusing web interfaces to control the view

Once the adversary has code execution in a browser, scripts will generally enumerate for vulnerable browser, extension and plug-in versions to prepare to the payload for arbitrary RCE.

Mitigations

Script/Ad Blockers (NoScript, uBlock, etc.)

Check for url hijacking(g00gle.com)

VirusTotal URL Checker

Stop clicking on everything

Web Developer? please sanitize all the inputs



Exploit Public Facing Applications

Applications, services and interfaces provide a direct path for an attacker to gain access to a system.

If the application is a website, access can then be leveraged to deliver subsequent attacks on the users of the site.

Bugs in software will forever be an attack vector, but many legitimate commands in applications can also be leveraged to obtain unexpected behavior.

CVE-2003-0201 Buffer Overflow for Samba <2.2.8a exploits an overflow condition in the call_trans2open to gain arbitrary code execution.

Mitigations

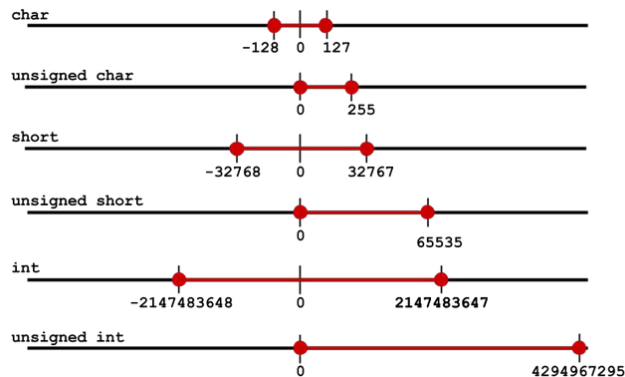
Keep your software updated

Also test your updates

Shut down any unnecessary services

Developer? Understand Secure Coding Practices

Watch out for Overflows & Race Conditions



Hardware Additions

Generally considered a physical vector, like walking up with a USB and achieving system access via autorun properties.

A technique of both low level penetration testers and nation state APTs. Stuxnet was originally delivered on a USB to an air-gapped network.

Can also include implanting hotspots (evil twin), sniffers (for MITM), or other techniques to impersonate or otherwise leverage hardware trust relationships.

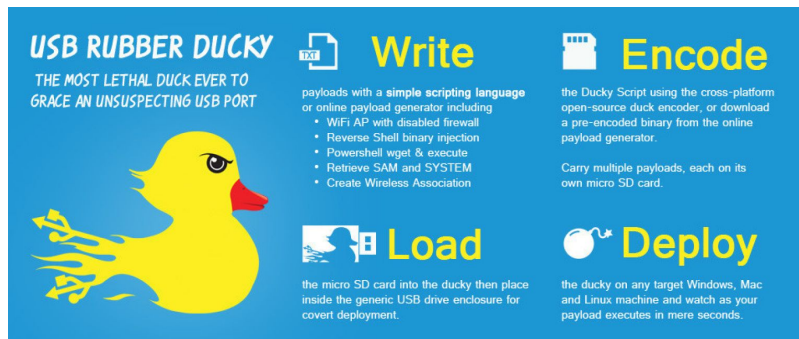
Mitigations

Don't plug things in randomly


Configure your systems to prevent autorun

Conduct site inspections regularly


Inspect network topologies for errant nodes




USB RUBBER DUCKY
THE MOST LETHAL DUCK EVER TO
GRACE AN UNSUSPECTING USB PORT


 **Write**
payloads with a **simple scripting language** or online payload generator including

- WIFI AP with disabled firewall
- Reverse Shell binary injection
- Powershell wget & execute
- Retrieve SAM and SYSTEM
- Create Wireless Association

 **Encode**
the Ducky Script using the cross-platform open-source duck encoder, or download a pre-encoded binary from the online payload generator.

Carry multiple payloads, each on its own micro SD card.

 **Load**
the micro SD card into the ducky then place inside the generic USB drive enclosure for covert deployment.

 **Deploy**
the ducky on any target Windows, Mac and Linux machine and watch as your payload executes in mere seconds.

Replication Through Removable Media

Similar to Hardware Additions, a means of propagating through a network that may involve a malware replicating itself onto physical devices

A given system that a malware exists on may not be vulnerable or the final target, so this could be a tactic of lateral movement or initial access.

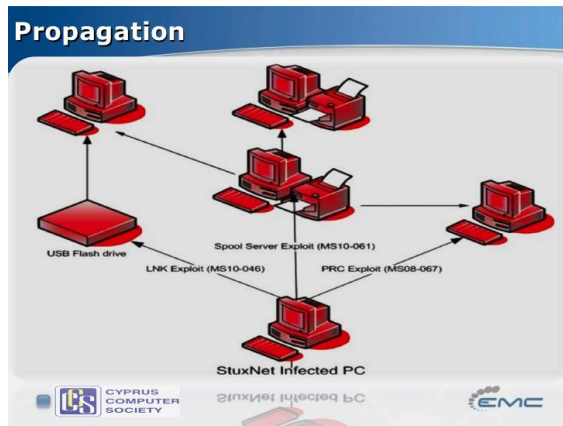
This was also a property of Stuxnet which it used to propagate throughout the Natanz facility in order to target air-gapped centrifuges.

Mitigations

Don't plug things in randomly

Configure your systems to prevent autorun

Maintain acceptable use policies for media devices



Spear/Phishing via Links/Attachments/Services

Spearphishing is a targeted form of phishing that seeks to infect particularly vulnerable or interesting users via multiple methods.

Links and attachments usually require user interaction in order to execute, so generally are accompanied with a social engineering context.

Scenario: You are a hiring manager in charge of reviewing candidates. You receive a personal email from a candidate with a PDF attachment of his resume. Do you open it?

Mitigations

Don't. Click. On. Anything.

Zero width text expanding plugin

Advanced email client protections

Simulated Phishing for user training

Check source email for discrepancies

From: Amazon <management@mazoncanada.ca> on behalf of not an Amazon email address (note the missing A in Amazon)
To: @sheridanc.on.ca
Cc:
Subject: Suspension

amazon.com®

Dear Client,

Generic non-personalized greeting

We have sent you this e-mail, because we have strong reason to believe, your account has been used by someone else. In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter. We've locked your Amazon account, and you have 36 hours to verify it, or we have the right to terminate it.

To confirm your identity with us click the link below:

<https://www.amazon.com/exec/obidos/sign-in.html>

Sincerely,

Hovering over the link reveals it points to a non-Amazon site - "http://redirect-kereskedj.com"

The Amazon Associates Team



© 1996-2013, Amazon.com, Inc. or its affiliates

Supply Chain Compromise

Manipulation of products or product delivery mechanisms for the purpose of compromising an end user.

Source code manipulation, private key hijacking, counterfeit distribution, factory image infections, and even shipment interdiction are all a part of supply chain compromise.

Usage of this tactic often includes watering hole attacks and can be an identifying factor for APTs.

Mitigations

Maintain control of private keys used for software

Verify MD5 Hashes before running software

Establish relationships with distributors

Tamper-proof/evident shipping mechanisms



Trusted Relationships and Valid Accounts

Generally a social engineering technique, impersonating or masquerading as a trusted service provider to gain access to resources or information otherwise unobtainable by an attacker.

Once someone has acquired valid credentials to a system or service, it becomes more difficult to track and mitigate the damage that is possible. Brute forcing credentials is still valuable for this reason.

Scenario: You are an IT manager of a large SoC and one of your remote employees is requesting an unusual password reset procedure for an urgent purpose.

Mitigations

Don't trust blindly! Verify credentials

Enforce password requirements

Follow company security policies and guidelines





Thank You

pedrourbina.com