Injecting Trojans & Malicious Code Via Patch & Systems Management Tools

Steve Manzuik

Senior Security Analyst

Injecting Trojans & Malicious Code Via Patch & Systems Management Tools

Today's key topics

- *Patch & Systems Management*
- *Patch Management Methodologies*
- *Abusing the Systems*
- *A Better Way*
- *Summary & Wrap-up*
- *Q&A*

Topic #1 Patch & Systems Management

Key Points to present on this slide are

- ***Why Patch Management?***
- ***What are the Various Solutions (Vendors)***
- ***Architecture of the Average Patch Management Solution***

Topic #2 Patches Up Close

Key Points to present on this slide are

- ***Purpose of Microsoft Patches***
- ***Microsoft "Patch Tuesday"***
- ***Anatomy of a Microsoft Patch***
- ***Flaws in the Process***

Topic #3 Abusing the System

Key Points to present on this slide are

- ***What Gaps Exists in Current Processes***
- ***Leveraging These Gaps to '0wn' the System***
- ***Examples of Attack Vectors – Fooling the System***

Topic #4 The Trojan Patch

Key Points to present on this slide are

- ***PATCH WILL BE CONSIDERED LEGITIMATE BY THE SYSTEM.***
- ***Patch May in Fact Fix the Issue But Will Also Provide Malicious Access or Perform Malicious Tasks.***

Topic #5 A Better Way

Key Points to present on this slide are

- ***Defense Tactics***
- ***Every Attack Has a Defense***
- ***The Process (not the vendor) is the Problem***
- ***Detection, Compliance & Quarantine***

Summary Wrap-up

QUESTIONS?

Steve Manzuik

403.630.4297

steve.manzuik@configuresoft.com