Secure Guard Consulting

Thank You All!

- My name is Kaushal Kothari, President of Secure Guard Consulting.
- Questions? Please contact me!

Kaushal Kothari

515-229-5674

kkothari@sgcsecure.com

https://secureguardconsulting.com

Secure Guard Consulting

Cybersecurity and IT Audit

About Me

- Certified Ethical Hacker
- Former FDIC IT Examination Analyst
- 20+ years of technology experience

(515) 229-5674 kkothari@sgcsecure.com

Goal – Value

- Current Exam Trends
- What is a Zero Day Attack
- Web Shell Demo
- What Happens After a Zero Day Attack?
- How Do We Protect Against Them?
- MITRE ATT&CK Framework – What Is It? Why Is It Important?

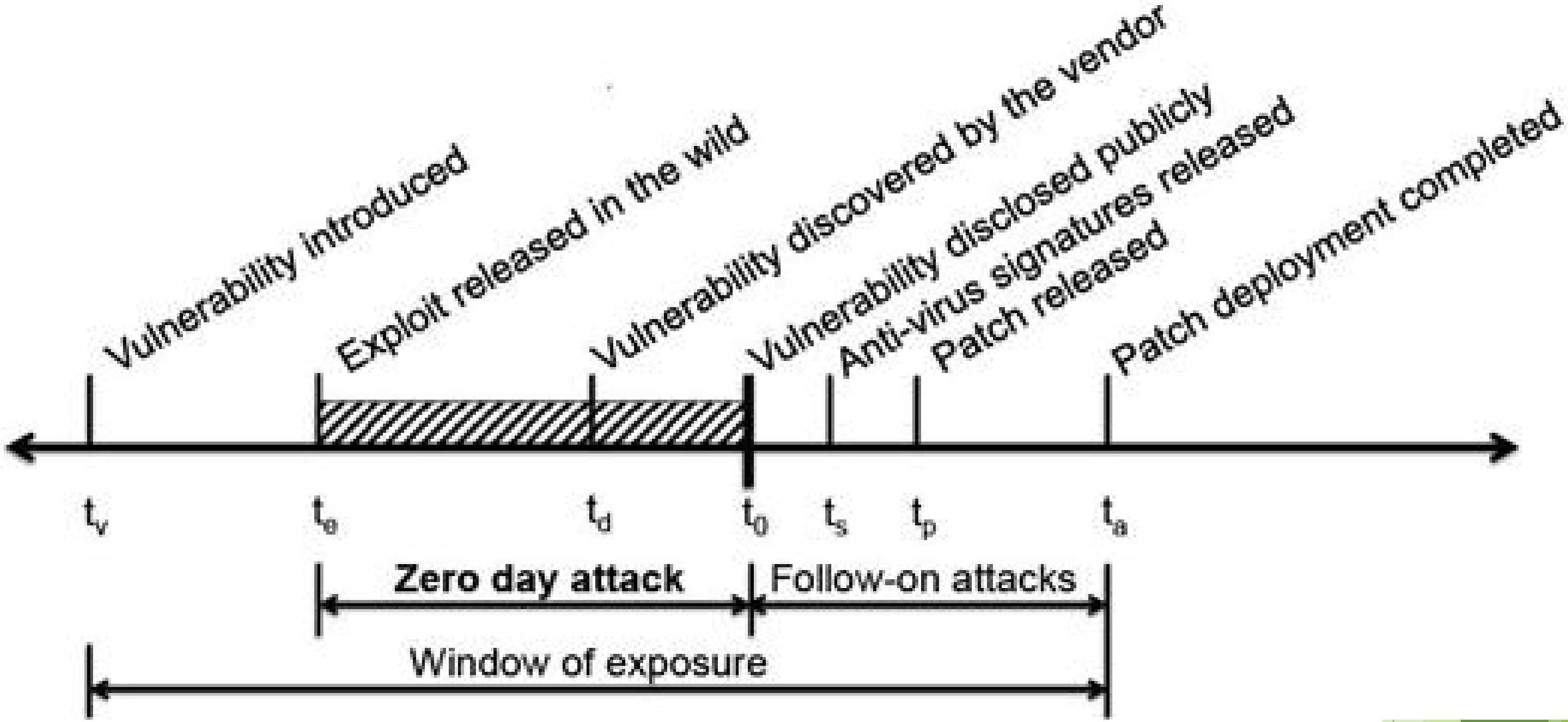
(515) 229-5674 kkothari@sgcsecure.com

Current Exam Trends

- User access reviews – not just core system
- System hardening procedures
- Social Media
- EOL – switches and routers
- * Ransomware *
  - MFA on admin access
  - Backups – air gapped or immutable backups
- Remote Access
  - MFA on remote access
  - Monitoring employee remote access
  - Time of day restrictions for remote access
- Vendor management
  - Ask your vendors with customer information how they responded and were they impacted by Exchange Zero Day
- Audits need to specify what they looked at – ours does this ☺

Zero Day Vulnerability

- Zero day vulnerability, zero day exploit, zero day attack (zero day)
  - Basically – I've developed software (e.g., Example App 1) and hackers have identified an exploitable vulnerability I don't know about. They are now attacking it. Upon seeing the attack, I now have "zero days" to fix it.
- The window of exposure for vulnerabilities is between the time when the **vulnerability is discovered** (by the criminal underground or ethical hackers) and a patch is released and **deployed onto systems**.


Vulnerability introduced
Exploit released in the wild
Vulnerability discovered by the vendor
Vulnerability disclosed publicly
Anti-virus signatures released
Patch released
Patch deployment completed
t_v
t_e
t_d
t_0
t_s
t_p
t_a
Zero day attack
Follow-on attacks
Window of exposure

Some studies show that the average window of exposure for a zero-day attack is ten months!

Exposure

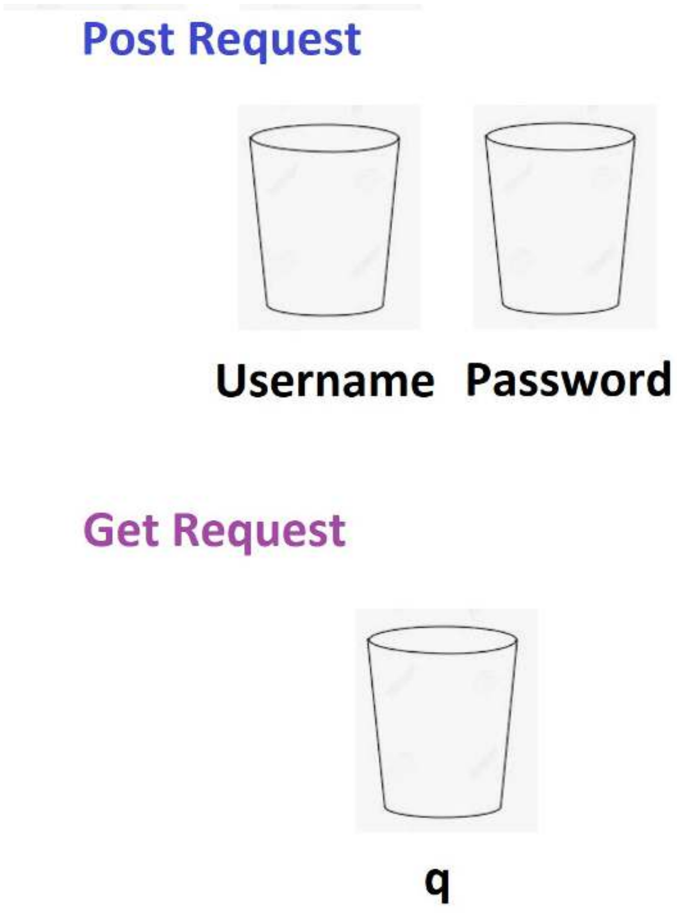
- Let’s extend the definition further …
  - the vendor has identified a vulnerability (e.g., Microsoft) and we have zero days to patch once it’s released.
  - Exposure is time between when released and when patched with hackers reverse engineering patches somewhere in between.
- A Quick Reminder
  - Any identified zero day attack, if that attack exists on an Internet accessible device, should be patched IMMEDIATELY, even at the cost of operations.

Examples

- Stuxnet
- Sony
- Heartbleed
- RSA
- **Exchange Zero Day**
- When it comes to Zero Day Attacks, it really doesn’t matter how the zero day worked …
- What matters is what happens after the breach.
- **Demo**

Web Shell

- Variables
  - Variables are a way to store information to use later in a program or send to a different page.



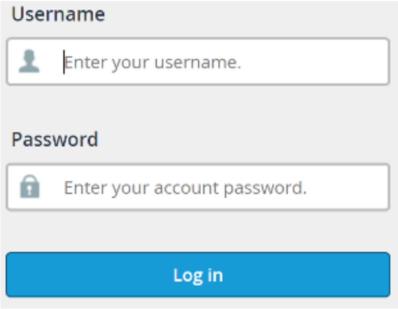
Post Request

Username Password

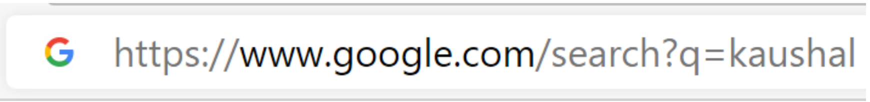
Get Request

q

- On Internet – 2 types of requests are made.
  - POST: Username and password – we can’t see them being submitted



  - GET: Google search



https://www.google.com/search?q=kaushal

Zero Day Breaches

- What happens after a zero day is breached?
  - Escalation of privileges
  - Lateral movement
  - Using Procdump and Mimikatz to capture password hashes
  - Use Powershell
- Procdump and Powershell are legitimate tools.
  - Abusable features
- Mimikatz can run in memory
  - Fileless attacks
- Both can essentially render traditional AV useless.

New threat Environment

- This is the new threat environment.
- Zero-day threats are only in the beginning stages.
- If the history of vulnerabilities and exploits is any indicator, zero-day threats will progressively get worse and present the biggest challenge to guard against.
- Hackers obtaining footholds into our networks.

Enter Next Generation Antivirus (NGAV) / Endpoint Detection and Response (EDR)

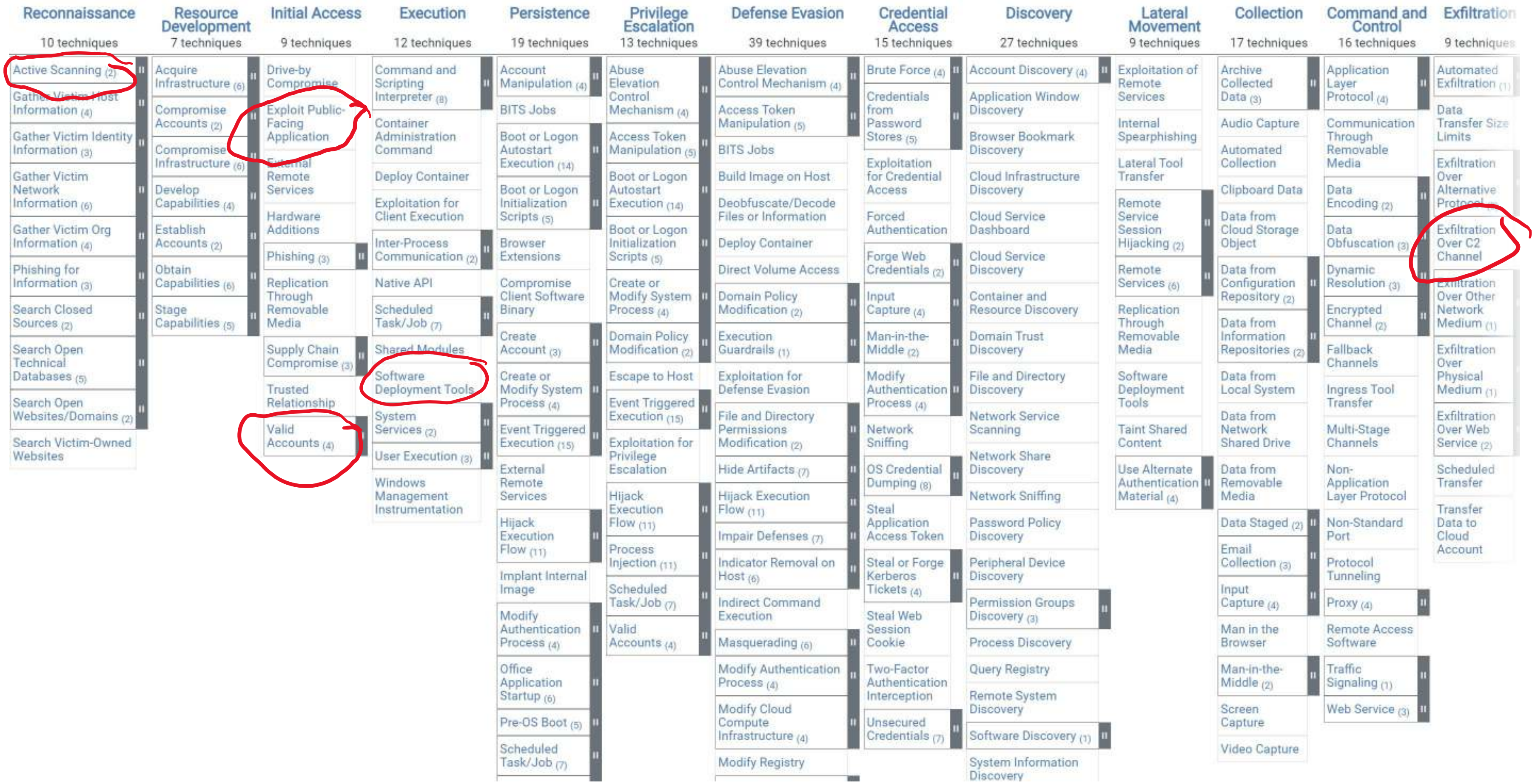
- The R is for Response
- Indicators of Compromise (IoC) vs Indicators of Attack (IoA)
  - Indicators of Compromise
    - Come in one morning and the vault is open and cash is missing.
  - Indicators of Attack
    - Thief cases the bank (reconnaissance)
    - Identifies time and best entry point
    - Breaks in at night
    - Disables security system
    - Brute forces combination
- SentinelOne, Crowdstrike, Sophos Intercept-X Advanced EDR

MITRE ATT&CK

- “is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target”
- In short – well organized knowledge base of tactics bad guys use to hack.
- https://attack.mitre.org/
- NGAV / EDR should address the MITRE ATT&CK

Mapping MITRE ATT&CK to Exchange Zero Day

- Reconnaissance
  - T1595 – Active Scanning
    - Scanning web for exposed Exchange Servers
- Initial Access
  - T1190 – Exploit Public-Facing Application
  - T1078 – Valid Accounts
    - The zero day allowed System privileges
- Execution
  - T1072 – Software Deployment Tools
    - Ability to write files on the exploited servers
- Persistence
  - T1505.003 – Server Software Component
    - Web Shell
- Exfiltration
  - T1041 – Exfiltration over C2 channel
    - Stealing email data for exploited organization
    - Stealing password hashes



Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques	Credential Access 15 techniques	Discovery 27 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration (1)
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (5)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (3)	Exfiltration Over C2 Channel
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)	Browser Extensions	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Dashboard	Remote Services (6)	Data from Cloud Storage Object	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (2)	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (7)	Create Account (3)	Escape to Host	Direct Volume Access	Man-in-the-Middle (2)	Container and Resource Discovery	Software Deployment Tools	Data from Information Repositories (2)	Fallback Channels	Exfiltration Over Web Service (2)
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules	Create or Modify System Process (4)	Event Triggered Execution (15)	Domain Policy Modification (2)	Modify Authentication Process (4)	Domain Trust Discovery	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Scheduled Transfer
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools	Event Triggered Execution (15)	Exploitation for Privilege Escalation	Execution Guardrails (1)	Network Sniffing	File and Directory Discovery	Use Alternate Authentication Material (4)	Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account
Search Victim-Owned Websites			System Services (2)	External Remote Services	Hijack Execution Flow (11)	Exploitation for Defense Evasion	OS Credential Dumping (8)	Network Service Scanning		Data from Removable Media	Non-Application Layer Protocol	
			User Execution (3)	Hijack Execution Flow (11)	Process Injection (11)	File and Directory Permissions Modification (2)	Steal Application Access Token	Network Share Discovery		Data Staged (2)	Non-Standard Port	
			Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job (7)	Hide Artifacts (7)	Steal or Forge Kerberos Tickets (4)	Network Sniffing		Email Collection (3)	Protocol Tunneling	
				Modify Authentication Process (4)	Valid Accounts (4)	Hijack Execution Flow (11)	Steal Web Session Cookie	Password Policy Discovery		Input Capture (4)	Proxy (4)	
				Office Application Startup (6)		Impair Defenses (7)	Two-Factor Authentication Interception	Peripheral Device Discovery		Man in the Browser	Remote Access Software	
				Pre-OS Boot (5)		Indicator Removal on Host (6)	Unsecured Credentials (7)	Permission Groups Discovery (3)		Man-in-the-Middle (2)	Traffic Signaling (1)	
				Scheduled Task/Job (7)		Indirect Command Execution		Process Discovery		Screen Capture	Web Service (3)	
						Masquerading (6)		Query Registry		Video Capture		
						Modify Authentication Process (4)		Remote System Discovery				
						Modify Cloud Compute Infrastructure (4)		Software Discovery (1)				
						Modify Registry		System Information Discovery				

Detecting a Zero-Day Compromise

- Behavior-based systems (IDS and IPS) alerts
- Antivirus software alerts as a result of heuristic scanning
- Unusual events in the system log files (i.e. failed logons)
- Poor system performance
- Unexplained system reboots
- Network traffic on unexpected ports, especially on ports known to be backdoor
- ports for known blended threats (i.e. MyDoom: TCP ports 3127 through 3198)
- Increased network traffic on a legitimate port
- Increased scanning activity
- Unusual SMTP traffic, especially originating from systems that should not be using SMTP

Alert Fatigue

- Alerting allows infections to happen.
- Which of the 1,000 alerts do you pay attention to?
- Most, if not all, threats and violations must be automatically blocked.