SightGain

TOP 10 THREATS

www.sightgain.com

TOP 10 THREATS

The following list represents the Top 10 Threats that SightGain partner Red Canary has observed in their customer environments over the last year. Each technique is actively exploited in the wild and therefore represents a high priority for protection activity. While there are Atomic Tests of these techniques that can be run manually, SightGain has included them in our automated testing tool available to everyone.

WHY STOP AT 10?

We're pragmatic at SightGain. This list is the best start an organization can use because it represents the threats that are happening most often. We have automated the testing of these techniques to make sure your controls are protecting, detecting, alerting, and responding as expected across the most common exploits. Once you are confident you are detecting and eliminating these threats, we recommend looking at industry specific threats and the latest threats observed in the wild. We can test those too once you get past the top 10.

SUMMARY

Here is a list of the Top 10 Threats that our partners have seen in their customers 2021. Click on the hyperlink to see details and understand what we would assess against the various techniques. Each link explains the technique, how to gain visibility, where to collect sources of detection, understand detection analytics, and the shows the manual Atomic tests of this technique.

Measuring yourself against the most used attack techniques is a good way to start and manage a security program. Here is a graphical overview of these techniques plotted against MITRE ATT&CK.

1. **Command and Scripting Interpreter**
   MITRE ATT&CK Technique T1059
2. **Signed Binary Proxy Execution**
   MITRE ATT&CK Technique T1218
3. **Windows Management Instrumentation**
   MITRE ATT&CK Technique T1047
4. **Credential Dumping**
   MITRE ATT&CK Technique T1003
5. **Ingress Tool Transfer**
   MITRE ATT&CK Technique T1105
6. **Process Injection**
   MITRE ATT&CK Technique T1055
7. **Scheduled Task/Job**
   MITRE ATT&CK Technique T1053
8. **Obfuscated Files or Information**
   MITRE ATT&CK Technique T1027
9. **Masquerading**
   MITRE ATT&CK Technique T1036
10. **Hijack Execution Flow**
    MITRE ATT&CK Technique T1574

Execution	Privilege Escalation	Defense Evasion	Credential Access	Command & Control
Command and Scripting Interpreter	Process Injection	Abuse Elevation Control Mechanism	OS Credential Dumping	Ingress Tool Transfer
Container Administration Command	Scheduled Task/Job	Hijack Execution Flow	Advesary-in-the-middle	Application Layer Protocol
Deploy Container	Abuse Elevation Control Mechanism	Masquerading	Brute Force	Communication Through Removable Media
Exploitation for Client Execution	Access Token Manipulation	Obfuscated Files or Information	Credentials from Password Stores	Data Encoding
Inter-Process Communication	Boot or Logon Autostart Execution	Access Token Manipulation	Exploitation for Credential Access	Data Obfuscation
Native API	Boot or Logon Initialization Scripts	BITS Jobs	Forced Authentication	Dynamic Resolution
Scheduled Task/Job	Create or Modify System Process	Deobfuscate/decode files or Information	Forge Web Credentials	Encrypted Channel
Shared Modules	Domain Policy Modification	Hijack Execution Flow	Input Capture	Fallback Channels
Software Deployment Tools	Escape to Host	Deploy Container	Modify \ Authentication Process	Multi-Stage Channels
System Service	Event Triggered Execution	Direct Volume Acccess	Network Sniffing	Non-Application Layer Protocol
User Execution	Exploitation for Privilege Escalation	Execution Guardrails	Steal Application Access Token	Non-Standard Port
	Hijack Execution Flow	Exploitation for Defense Evasion	Steal or Forge Kerberros Tickets	Protocol Tunneling
	Valid Accounts	File and Directory Permissions Modificiation	Steal Web Session Cookie	Proxy
		Hide Artifacts	Two-Factor Authentication Interception	Remote Access Software
		Hijack Execution Flow	Unsecured Credentials	Traffic Sniffing
				Web Service

The MITRE ATT&CK matrix lays out the tactics that malicious actors need to follow to exfiltrate or otherwise impact their targets. They are typically caught attempting to compromise native operating system utilities to execute code or bring in custom tooling. Or they are caught elevating privilege levels to get further access to compromised systems. We also catch them working to get persistence access and manipulating customers' defensive controls to evade prevention or detection. These are necessary means to their end goal—if organizations disrupt these initial activities, they can prevent data theft, ransomware, or other actions malicious actors attempt to implement. Most security practitioners know that if we stop tactics early on in this process, malicious actors will not be able to reach their goal. The above graphic bears this out as there are earlier ATT&CK tactics observed than later ones.

CONCLUSION

At SightGain we know that a lot must go right for security to work. Oftentimes, things are not working the way they seem and fail to adequately prevent, detect, and respond the threats. Therefore, it is more important than ever to make sure you are proactively testing your responses and tuning your system to ensure that it is providing the best possible outcomes. SightGain makes that testing and tuning easy.

SightGain

SightGain's Continuous Readiness Platform is designed to find gaps and redundancies in the performance of people, processes, and technology in cybersecurity systems. It uses live-fire attack simulations to measure, quantify, and optimize cyber defense readiness.

www.sightgain.com