

04/02/2022



XDR Overview

Detection & Forensic Investigation

404 Wyman Street
Suite 357
Waltham, MA 02451
www.uptycs.com

Uptycs XDR covers 4 types of detections:

- **Behavioral:** Scan for MITRE ATT&CK techniques
- **Contextual:** YARA scan of process memory and files
- **IOCs:** Match against threat intelligence to identify known-bad indicators such as domains, IPs, file hashes, and JA3 fingerprints
- **Advanced:** Scan for advanced attacks including Process Hollowing and DLL Injection

Uptycs XDR also includes key forensic investigation capabilities:

- **Detailed historic telemetry** available for further analysis, even if endpoint is offline
- Ability to **carve files and memory** from endpoints in real-time
- Ability to **scan files and memory** with YARA rules in real-time

Behavioral Detections	
What Is It?	Mapping to the MITRE ATT&CK Framework and analyzing behavior to detect various techniques and sub-techniques used in execution, persistence, privilege escalation, lateral movement, and more.
Differentiating Features	<ul style="list-style-type: none"> • Pre-built library of 1,000+ event and alert rules that cover 180+ MITRE ATT&CK techniques across Windows, Linux, and macOS • Ability to add custom behavioral rules • Correlation engine to link multiple alerts and events into a single detection, to reduce alert fatigue & accelerate triaging • Detection of lateral movement by looking at remote login activity related to suspicious / malicious events • Monitoring of file events via built-in FIM capabilities • Ability to tune rules to environment by adding exceptions • Built-in workflow management tools (Assign, Add Notes, Close)
Advantages	<ol style="list-style-type: none"> 1. By focussing on suspicious activities Uptycs can uncover actual attacker (human) activity, in addition to the malware involved e.g if an attacker wants to use net.exe to add a user we can detect it 2. Through a behavior-based approach, Security Analyst can easily arrive at a baseline of alerts normally seen in his organization's environment and identify abnormalities requiring deeper introspection 3. Behavioral detection of threats round-the-clock forms the basis for Threat Hunting and Continuous Compliance

Examples

<p>Windows OS</p>	<p>ATTACK_INHIBIT_SYSTEM_RECOVERY_T1490_WINDOWS_LOLBAS_VSSADMIN - Vssadmin.exe execution detected for deleting shadow copies - T1490 - Inhibit System Recovery - Windows</p> <p>ATTACK_DEOBFUSCATE_DECODE_FILES_OR_INFORMATION_T1140_WINDOWS_LOLBAS_DOWNLOAD_DECODE_CERTUTIL - Certutil.exe execution detected to download and decode data - T1140 - Deobfuscate/Decode Files or Information - Windows</p> <p>ATTACK_EXECUTION_T1560_WINDOWS_EXECUTABLE_FIM_LATERAL_SYSTEM - Likely remote system process dropped portable executable file - T1570 - Lateral Movement - Windows</p>
<p>MacOS</p>	<p>ATTACK_CREDENTIAL_DUMP_T1555_MACOS_KEYCHAIN_MODIFY - Keychain file dumped to disk - T1555 Credential Dumping for macOS</p> <p>ATTACK_PERSISTENCE_T1037_MACOS_BOOT_OR_LOGON_FILE - Process added Boot or Logon Initialization Scripts - T1037 Persistence for macOS</p> <p>ATTACK_PERSISTENCE_T1159_MACOS_FILE_PLIST_LAUNCHDAEMONS - Process created plist file in LaunchDaemons - T1159 Persistence for macOS</p>
<p>Linux</p>	<p>ATTACK_CREDENTIAL_ACCESS_T1110.001_LINUX_PASSWORD_GUESSING - Password guessing detected - T1110.001 Credential Access Linux</p> <p>ATTACK_IMPAIR_DEFENSE_T1562.004_LINUX_DISABLE_MODIFY_FIREWALL - Process or script trying to alter firewall rules - T1562.004 Impair Defense Modify Firewall_LINUX</p> <p>ATTACK_PRIVILEGE_ESCALATION_T1548.003_LINUX_MODIFY_SUDO_CONFIGURATION - Process trying to modify sudo configuration - T1548.003 Privilege escalation_LINUX</p>

Contextual Detections	
What Is It?	Use YARA scanning for malware / toolkit detection based on rules curated by the Uptycs Threat Research and enriched with intel on top APT groups
Malware Covered	220+
APT Threat Actors	30+
Differentiating Features	<ul style="list-style-type: none"> Uptycs performs highly optimized process memory scans on Windows and Linux endpoints/hosts to identify malware <ul style="list-style-type: none"> Scans are conducted on every new process that stays alive for 5 seconds (configurable) or more Scans are done on specific regions of memory to reduce asset overhead For any OS that doesn't support process memory scan (e.g MacOS), process file scan is conducted on the binary based on the YARA rule Ability for user to define custom YARA scan rules
Examples	
Mimikatz	Mimikatz is a post-exploitation tool that dumps passwords from memory and enables lateral movement within a network. <i>(rule Uptycs_Mimikatz)</i>
Whispergate	Whispergate is a wiper targeting Ukraine which overwrites the MBR (Master Boot Record) and files. <i>(rule Uptycs_Whispergate)</i>
Coinminer	Coin miner is an application that uses the infected device's physical resources to mine digital currency. <i>(rule Uptycs_Coinminer)</i>
Sysjoker	Sysjoker is a multi platform backdoor which targets windows, mac and linux operating systems. <i>(rule Uptycs_Sysjoker)</i>
PenguinTurla	PenguinTurla is a linux malware that maintains stealth without requiring elevated privileges while running arbitrary remote command. <i>(rule Uptycs_PenguinTurla)</i>

IOC Detections	
What Is It?	Look for indicators of compromise in real-time and historical data (via Threat Books), using a pre-curated list of indicators from Uptycs Threat Research team or custom lists uploadable by users.
Indicators	~6M across 7 categories (e.g. malware, coinminer, phishing, DGA, unrecognized website)
Indicator Types	<ul style="list-style-type: none"> • Domain • IP • File hash • JA3 fingerprint
Differentiating Features	<ul style="list-style-type: none"> • Intelligence feed curated by Uptycs Threat Research team using open-source intel and primary research (sandbox analysis) • Daily updates to intelligence feed • Ad Hoc threat intelligence feed update support • Threat Books: Ability to look for new attacks with specific IoCs in historical data • Pre-built Threat Books for active campaigns • Ability to add custom indicators • Integration with VirusTotal
Advantages	<ol style="list-style-type: none"> 1. Curated intelligence from various sources allows for real-time alerts to be generated on most current threat indicators 2. Deeper detection intelligence by extracting additional insights (metadata) on potential malware via sandbox 3. Substantial reduction of false positives daily through automation, allow-list data from reliable sources, passive DNS data, and manual validation by the Uptycs threat intelligence team
Examples	
AsyncRAT	Through a simple email phishing tactic with an HTML attachment, threat attackers are delivering AsyncRAT designed to remotely monitor and control its infected computers through a secure, encrypted connection. This campaign has been in effect for a period of 4 to 5 months.
COVID Omicron	Threat actors don't shy away from using misery and fear to their advantage. FortiGuard Labs recently came across a curiously named file, "Omicron Stats.exe", which turned out to be a variant of Redline Stealer malware.

Advanced Detections (Beta)	
What Is It?	Detection of advanced attacks (e.g. Ransomware, Keylogging) on the endpoint using correlation of system API calls.
Advanced Techniques	<ul style="list-style-type: none"> • Clipboard stealing • Credential dumping • DLL injection • Keylogger • MBR Attack • Process Hollowing • Ransomware • Token Impersonation
Differentiating Features	<ul style="list-style-type: none"> • Logic built into endpoint agent to rapidly detect advanced attacks • Ability to intervene and block attacks in certain scenarios
Examples	
DLL Injection	Detection of a process is trying to load its code in another process via forced loading of a shared library, e.g. LD_PRELOAD on Linux
Process Hollowing	Detection when a process creates another in a suspended state, unmaps (hollows) its memory, and replaced with different (malicious) code

Remediation & Blocking

Remediation Capability	Linux	MacOS	Windows
Process			
Pause / Resume Process	X	X	X
Kill Process	X	X	X
Kill container (Roadmap 2022)	(Q1)		
Networking			
Quarantine / Un-quarantine	X	X	X
Firewall rules	X		X
File			
Delete	X	X	X
Permissions update (UI support TBD)	X	X	
Undelete (Roadmap 2022)			(Q1)
Registry			
Delete			X

Remediation Capability	Linux	MacOS	Windows
Run Script			
Run Script ¹	X	X	X
Users			
Enable / Disable	X	X	X
Services			
Enable / Disable	X		X
Restart / Start / Stop			X
Host			
Reboot / Shutdown	X	X	X
Restart osquery	X	X	X
Force Config Refresh for osquery	X	X	X

Footnotes:

1. Scripts can be used for a diverse set of remediation steps e.g. downloading a hotfix & applying, finding all instances of a file and deleting, etc.

Blocking Capability	Linux	MacOS	Windows
Process (Block / Allow / Log)			
Path Regex Match	X	X	X
File Hash Match	X	X	X
Signing Certificate Hash Match		X	X
Yara Match (Roadmap 2022)	(Q1)	(Q1)	(Q1)
DNS (Block)			
Domain Match		X	