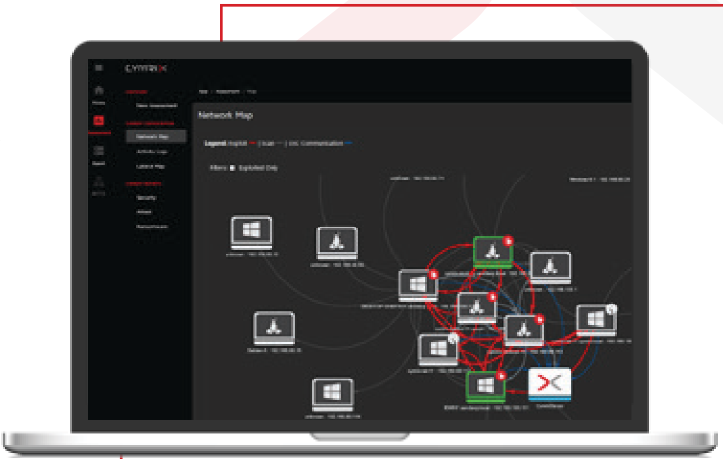
How can you improve your cybersecurity resilience?

Ransomware is an increasingly prevalent and profitable threat. There are already more than 400 families of ransomware, and the number is growing. At the same time, ransomware is getting smarter, more expensive, and more targeted, so attacks are getting worse.

The annual Security Outcomes Report from Cisco shows that 96% of executives think security resilience is very important. As organizations try to protect themselves from rapidly evolving threats, they will need to use **offensive security skills to think like attackers and get ahead of them**. Conducting regular Cyber Breach and Attack Simulations can provide critical insight into potential vulnerabilities and assist in prioritizing where to spend valuable time and resources.

> *93% of our ransomware incident response engagements revealed insufficient controls on privilege access and lateral movement*
> *–Microsoft Digital Defense Report 2022*



What is Cymrix?

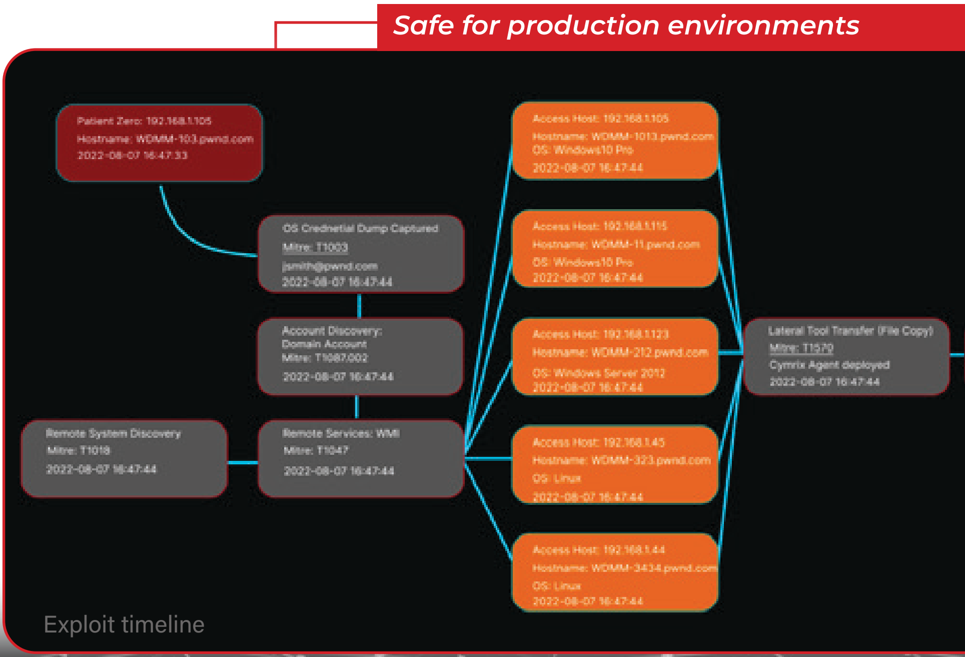
Through reverse engineering and the de-weaponization of authentic malware samples, Cymrix is designed to safely simulate a ransomware infection on your organization’s network. Following the MITRE ATT&CK framework, Cymrix finds and fingerprints internal attack surfaces, identifies exploitable vulnerabilities, incorrect configurations, obtainable credentials, and product defaults from the perspective of a real-world hacker.

It begins by installing a lightweight agent on “Patient Zero” and then uses the same Tools, Techniques, and Procedures (TTPs) that a real attackers leverage to compromise environments. As Cymrix propagates throughout the network, it tracks and records critical data and systems, sensitive or regulated network segments, and operational single points of failure.

Cymrix’s reporting feature details a step by step lateral attack path and provides your organization with a visual roadmap to remediate data separation, network segmentation, and user permissions. This level of understanding allows your team to build a program that goes beyond testing, patching, and threat hunting.

True resiliency is achievable with Cymrix. Let us show you how.

Safe for production environments



Patient Zero: 192.168.1.105
Hostname: WDMM-103.pwnd.com
2022-08-07 16:47:33

OS Crednetial Dump Captured
Mitre: T1003
jsmith@pwnd.com
2022-08-07 16:47:44

Account Discovery:
Domain Account
Mitre: T1087.002
2022-08-07 16:47:44

Remote System Discovery
Mitre: T1018
2022-08-07 16:47:44

Remote Services: WMI
Mitre: T1047
2022-08-07 16:47:44

Access Host: 192.168.1.105
Hostname: WDMM-1013.pwnd.com
OS: Windows10 Pro
2022-08-07 16:47:44

Access Host: 192.168.1.115
Hostname: WDMM-11.pwnd.com
OS: Windows10 Pro
2022-08-07 16:47:44

Access Host: 192.168.1.123
Hostname: WDMM-212.pwnd.com
OS: Windows Server 2012
2022-08-07 16:47:44

Access Host: 192.168.1.45
Hostname: WDMM-323.pwnd.com
OS: Linux
2022-08-07 16:47:44

Access Host: 192.168.1.44
Hostname: WDMM-3434.pwnd.com
OS: Linux
2022-08-07 16:47:44

Lateral Tool Transfer (File Copy)
Mitre: T1570
Cymrix Agent deployed
2022-08-07 16:47:44

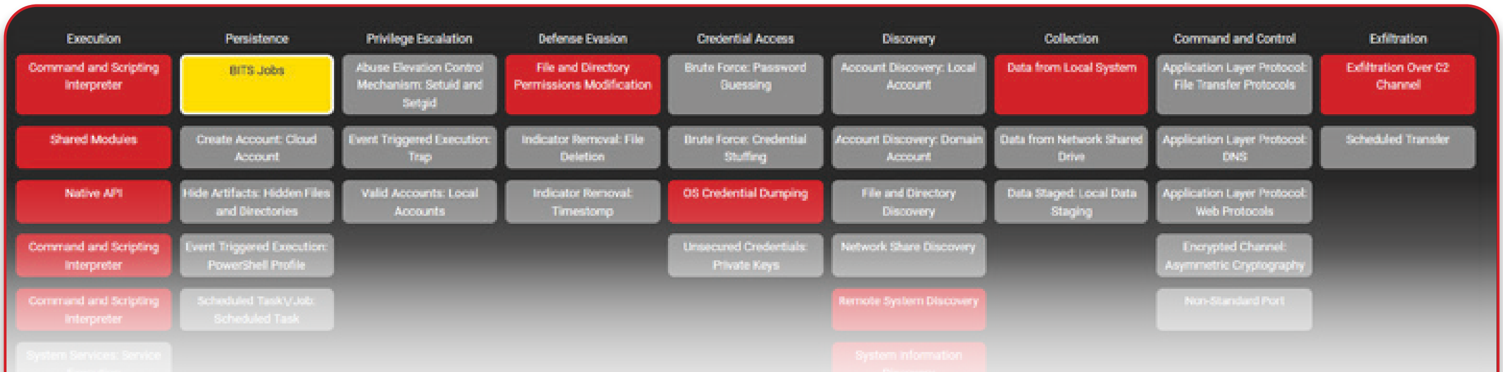
Exploit timeline

The Cymrix Ransomware Impact Analysis

Many organizations put a lot of focus on technical controls and attacks, but if they don't understand the environment as a whole, their efforts can often be wasted and ineffective. Our team uses Cymrix as part of a larger Ransomware Impact Assessment to help you spend your time on what's really important.

The Ransomware Impact Analysis (RIA) is a technology-enabled service that runs on a detailed breach and attack simulation platform made up of pre-built plays that match TTPs seen in real-world attack scenarios, such as combinations of ransomware and MITRE ATT&CK playbooks. An RIA provides your organization with a detailed list of vulnerabilities based on the attack path as well as a visual roadmap to remediate data separation, network segmentation, and user permissions, strengthening your security posture and hardening your environment against infection. The service includes:

- Interviews with key personnel and management to understand your organization's critical data and systems
- Review of preventive security controls that can reduce the likelihood of ransomware, such as strong authentication mechanisms and phishing training and awareness
- Running multiple live-fire ransomware simulations of defined network segments
- Providing a report with actionable recommendations to help your team reduce ransomware risk and strengthen your overall security posture
- Providing policy and strategy recommendations to limit the business impact if you do experience a ransomware attack



Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Collection	Command and Control	Exfiltration
Command and Scripting Interpreter	BITS Jobs	Abuse Elevation Control Mechanism: Setuid and Setgid	File and Directory Permissions Modification	Brute Force: Password Guessing	Account Discovery: Local Account	Data from Local System	Application Layer Protocol: File Transfer Protocols	Exfiltration Over C2 Channel
Shared Modules	Create Account: Cloud Account	Event Triggered Execution: Trap	Indicator Removal: File Deletion	Brute Force: Credential Stuffing	Account Discovery: Domain Account	Data from Network Shared Drive	Application Layer Protocol: DNS	Scheduled Transfer
Native API	Hide Artifacts: Hidden Files and Directories	Valid Accounts: Local Accounts	Indicator Removal: Timestomp	OS Credential Dumping	File and Directory Discovery	Data Staged: Local Data Staging	Application Layer Protocol: Web Protocols	
Command and Scripting Interpreter	Event Triggered Execution: PowerShell Profile			Unsecured Credentials: Private Keys	Network Share Discovery		Encrypted Channel: Asymmetric Cryptography	
Command and Scripting Interpreter	Scheduled Task\/Job: Scheduled Task				Remote System Discovery		Non-Standard Port	
System Services: Service Execution					System Information Discovery			
					[illegible]			

The Simulation Exercise

Our team works closely with our clients to deploy and execute the Cymrix simulation agent on Patient-Zero(s). In a typical RIA, the simulations take place in three phases:

Phase One: Zero Knowledge

The simulation agent is executed with no knowledge of the internal environment. This is intended to simulate an attack by a well-known vector against the current security controls

Phase Two: Zero-Day

The simulation agent is "whitelisted" by the current security controls (endpoint security, EDR, antivirus etc...) for the purpose of simulating an attack utilizing a zero-day vulnerability or other vulnerabilities where there is no current defense

Phase Three: Captured Credentials

The simulation agent is provided with elevated credentials for the purpose of simulating an attack where the credentials of an admin level user have previously been captured