DR
JOYE
PURSER

SECURE SOFTWARE, INSIDE AND OUT

PICUS **RED REPORT** 2024

"Just as these [hunter-killer] subs move silently through deep waters and launch devastating attacks to defeat their targets' defenses, new malware is designed to not only evade security tools but actively bring them down."

Dr. Suleyman Ozarslan
Picus Security Co-founder and VP of Picus Labs

The most prevalent ATT&CK techniques identified in 2023, ordered by the percentage of malware samples which exhibited the behavior.

↑	#1 2023:4	32%	T1055 Process Injection Defense Evasion · Privilege Escalation
↓	#2 2023:1	28%	T1059 Command and Scripting Interpreter Execution
◆	#3 New	26%	T1562 Impair Defenses Defense Evasion
↑	#4 2023:5	23%	T1082 System Information Discovery Discovery
↓	#5 2023:3	21%	T1486 Data Encrypted for Impact Impact

PROCESS INJECTION

- Tactics: privilege escalation, defense evasion
- Inserting malicious code into a legitimate process, enabling the attacker to run their code in the context of that process.
- The strategy effectively masks the malicious activity, helping it to evade basic detection mechanisms
- Enables persistence and access to higher levels of privileges.

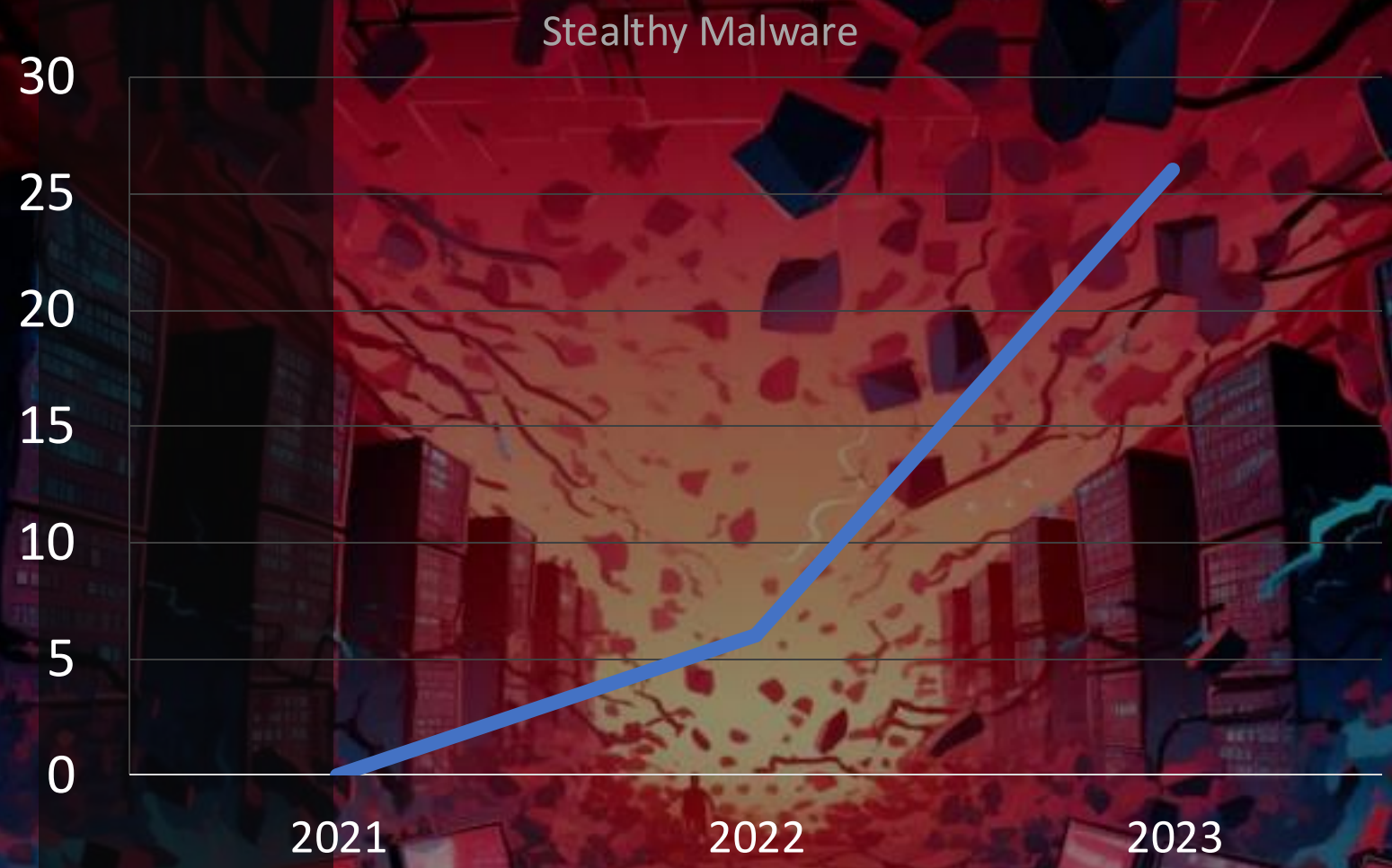
SYSTEM INFO DISCOVERY

- Threat actors collect information about computer systems, such as hardware, software, and network configurations.
- Adversaries use built-in tools to gather data on the network, seeking vulnerabilities to exploit.

IMPAIR DEFENSES: TACTICS

T1562.001 Disable or Modify Tools
T1562.002 Disable Windows Event Logging
T1562.003 Impair Command History Logging
T1562.004 Disable or Modify System Firewall
T1562.006 Indicator Blocking
T1562.007 Disable or Modify Cloud Firewall
T1562.008 Disable or Modify Cloud Logs
T1562.009 Safe Mode Boot
T1562.010 Downgrade Attack
T1562.011 Spoof Security Alerting
T1562.012 Disable or Modify Linux Audit System

DRAMATIC INCREASE IN MALWARE SPECIFICALLY TARGETING SECURITY CONTROLS



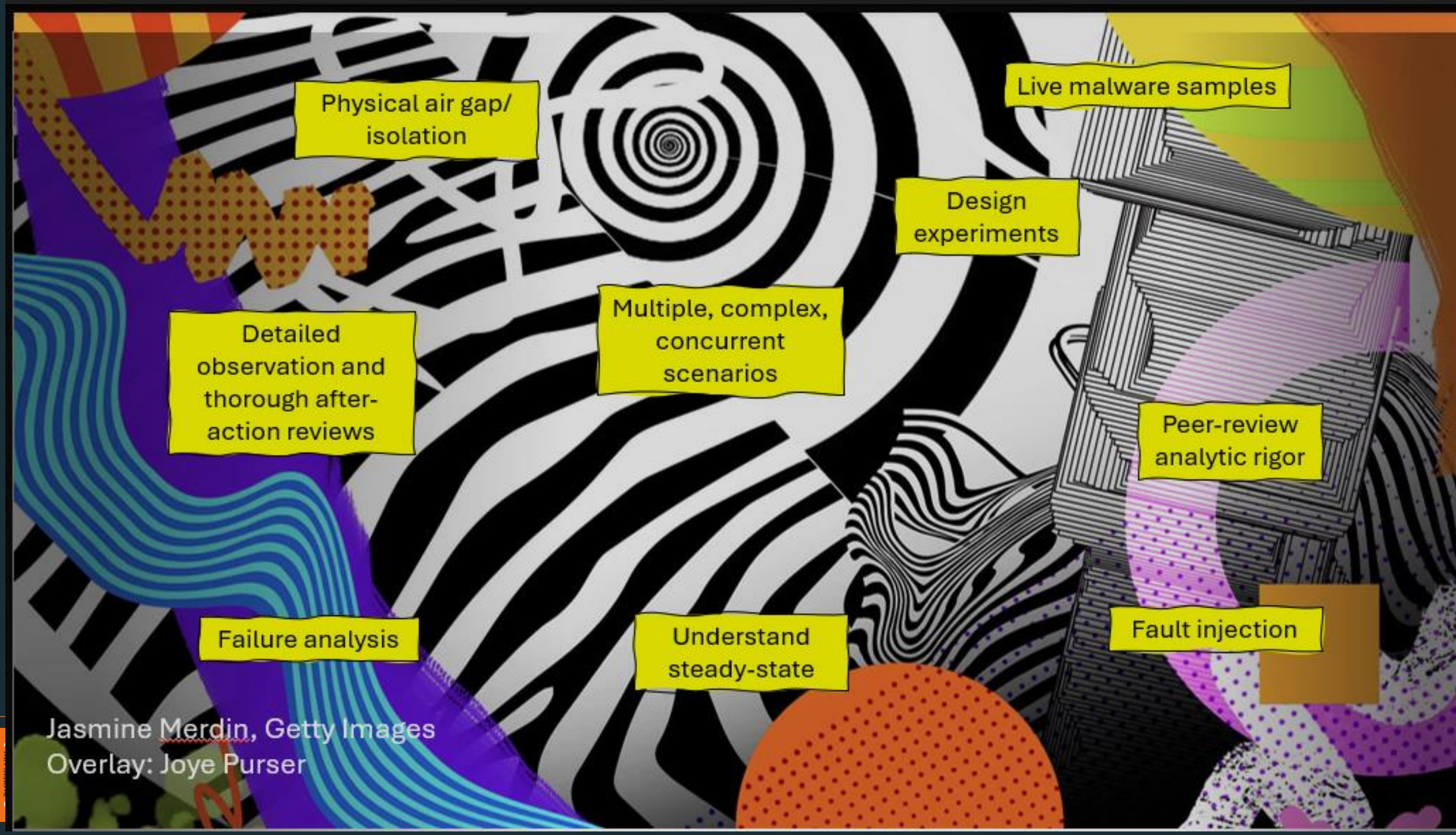
VERITAS FINDINGS

APPLICATION-TAILORED EXPLOIT.

- Threat actors are surveilling existing applications, targeting ones that result in the greatest “blast radius” following compromise.

ORGANIZATIONAL EXPLOIT.

- Anomaly detection tools fail to identify threat activity due to victim organization “stovepiping.”


Physical air gap/ isolation
Live malware samples
Design experiments
Multiple, complex, concurrent scenarios
Detailed observation and thorough after-action reviews
Peer-review analytic rigor
Failure analysis
Understand steady-state
Fault injection
Jasmine Merdin, Getty Images
Overlay: Joye Purser

SecDevOps:
Our Secure Software Development Process

Train
- General Security Training
- Role Specific Training
- *"PSG Presents"* Security Presentations
- Executive Order training via Tiger Team meetings

Requirements
- PubSec Requirements
- Data Classification
- Public, Restricted, High Restricted

Design
- Architectural Risk Analysis
- Threat Modeling
- Secure Design Principles
- Cryptography

Implement
- Secure Coding
- Static Code Analysis
- Secure Source Code Watermarking

Test
- Attack Surface Enumeration
- Dynamic Security Testing
- Penetration Testing
- REDLab

Deploy
- Third Party Component Security Review
- Packaging & Code Signing
- Secure by Default
- Securing Credentials
- Veritas Process Compliance

Maintain
- Vulnerability Management
- Third Party Monitoring
- Incident Response
- Patching
- Lifecycle Management (EOL)

Aligned with the US Government's Secure Software Development Framework (NIST SP 800-218) and Executive Order 14028

STRENGTHENING SECDEVOPS

- We perceive the Backup system becoming a prime target
- Veritas has created a “REDLab” where we set live malware loose: our own “cyber range”
- We fine-tune defense mechanisms, study new attack vectors, and adjust our software to protect against new threats

VERITAS

The REDLab

REDLab

- Study the injection of live malware variants in the Lab
- Perform independent research
- Validate resiliency of NetBackup solutions against Ransomware threats
- Validate customer data immutability
- Identify new attack vectors
- Update defense mechanisms monthly
- Leveraged RaaS and other malware sources
- Orchestrated PEN testing
- API Fuzz Testing

Filename	NBU	Anti Virus A	Anti Virus B	Anti Virus C	Anti Virus D
1.BIN	YES	HEUR/AGEN.1250041	Ransom.sorry	Ransom:MSIL/FileCoder.AD!MTB	YES
a91491f45b851a07f91ba5a200967921bf796d38677786de51a4a8fe5ddeafd2	YES	TR/Crypt.XPACK.Gen	ML.Attribute.HighConfidence	Ransom:Win32/Blocker	YES
BUILD.BIN	YES		Packed.Generic.525	Trojan:WIn32/RaccryptGL!MTB	YES
Proforma Invoice and Bank swift-REG.PI-0086547654. exe	YES	TR/Ransom.JB	Ransom.wannacry	Ransom:Win32/WannaCrypt	YES
f5fdebc5f4d3b970eb47606ddf51a71f0f6cb29068acb67c253efc0e959166	YES	TR/AD.Swotter.kjtqh	ML.Attribute.HighConfidence	Trojan:Win32/FormBook.SM!MTB	YES
GandCrab.BIN	YES	HEUR/AGEN.1223939	Packed.Generic.525	Trojan:Win32/Predator.DSK!MTB	YES
RIP_YOUR_PC_LOL.BIN	YES	HEUR/AGEN.1222682	Trojan.Gen.MBT	Ransom:Win32/WannaCrypt.A!rsm	YES
The_Czech_Republic_Chapter_of_the_ACFE-Invite.MSG	NO	Did NOT Detect	Did NOT Detect	Did NOT Detect	YES
VQ.DO	NO	Did NOT Detect	Did NOT Detect	Did NOT Detect	YES
wannaCry.INFECTED	YES	TR/Ransom.JB	Ransom.Wannacry	Ransom:Win32/WannaCrypt	YES
YourCyanide.CMD	NO	Did NOT Detect	Trojan.Gen.MBT	Trojan:Script/Wacatac.B!ml	YES

SecDevOps:
Our Secure Software Development Process

Train
- General Security Training
- Role Specific Training
- *"PSG Presents"* Security Presentations
- Executive Order training via Tiger Team meetings

Requirements
- PubSec Requirements
- Data Classification
- Public, Restricted, High Restricted

Design
- Architectural Risk Analysis
- Threat Modeling
- Secure Design Principles
- Cryptography

Implement
- Secure Coding
- Static Code Analysis
- Secure Source Code Watermarking

Test
- Attack Surface Enumeration
- Dynamic Security Testing
- Penetration Testing
- REDLab

Deploy
- Third Party Component Security Review
- Packaging & Code Signing
- Secure by Default
- Securing Credentials
- Veritas Process Compliance

Maintain
- Vulnerability Management
- Third Party Monitoring
- Incident Response
- Patching
- Lifecycle Management (EOL)

Aligned with the US Government's Secure Software Development Framework (NIST SP 800-218) and Executive Order 14028

Joye.Purser@veritas.com