
Achieving Cyber Vigilance in 2022
Tom Kellermann, Head of Cybersecurity Strategy
vmware

1


The Era of Cybercrime Cartels
vmware

2


Top Attack Vectors
• Ransomware via RAT
• Application Attacks
• Exploits against Microsoft and VPNs
• Island Hopping

3

Threat: Ransomware

Collection and Magnification

- **REvil**: originally known as "Sodinokibi"; Linux version released in 2021; shutdowns ESXi VMs before encryption; targeted by a coordinated take-down operation
- **DarkSide**: initially used REvil but now created their own ransomware; responsible for the Colonial Pipeline attack; evolved to target ESXi targets, and often deployed after vCenter access
- **BlackMatter**: evolution of DarkSide, possibly done as a way to distance themselves from the backlash created by the Colonial Pipeline attack
- **Defray**: also known as Defray777, explicitly target ESXi VMs, less sophisticated of other threats as binaries are not stripped of debugging symbols
- **HelloKitty**: yet another threat evolving from Windows to target Linux systems and ESXi servers; virtual machines are stopped before encryption; responsible for high profile attacks, like the one against CD ProjektRed
- **ViceSociety**: spin-off of HelloKitty, possibly from the same code base, and targeting SME businesses
- **Erebus**: old threat, Linux based, multi-language, apparently discontinue but with many component used by recent threats
- **GonnaCry**: open-source ransomware sample written in Python and C. "C" version actively used in the wild
- **eChOraix**: ransomware targeting QNAP NAS devices, written in GO, targeting end users rather than businesses

4

Linux Ransomware

Something wicked this way comes

- Targeted Ransomware attacks against cloud environments are often combined with data exfiltration, implementing a double-extortion scheme that improves their odds of success.
- Linux ransomware now targets host images used to spin up workloads.
- The detection of sophisticated Linux threats requires dynamic analysis and continuous host monitoring—capabilities that work well with the Linux kernel.

5

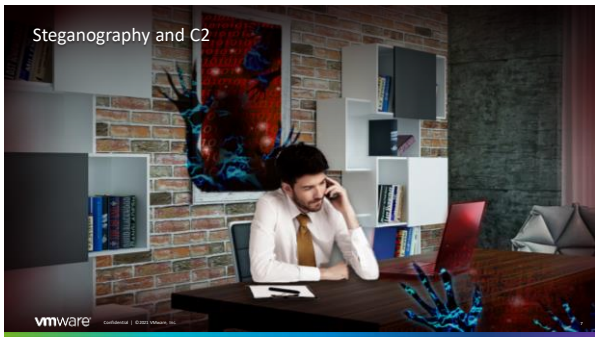
The Resurgence of RATS

The Top 3

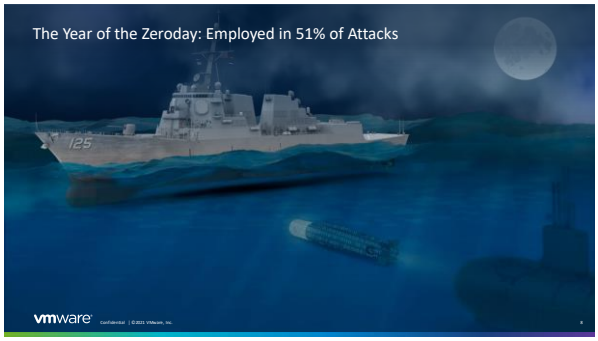
RATS entrench themselves within their infected systems to persist. They become background noise within a showing up as just another Windows service or application to operate undetected.

- **Vermilion Strike** is an open-source threat emulation software based upon Cobalt Strike's protocols, making it compatible with Cobalt Strike servers.
- ELF Plead is a Linux version of a RAT used by the threat actor 'BlackTech'. The configuration is RC4-encrypted, and a 32-byte encryption key can be found before the encrypted configuration. It uses a custom protocol to communicate with a C2 server.
- **Merlin**

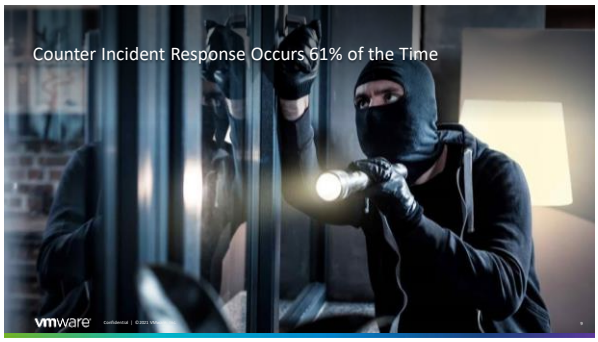
6


Steganography and C2
vmware

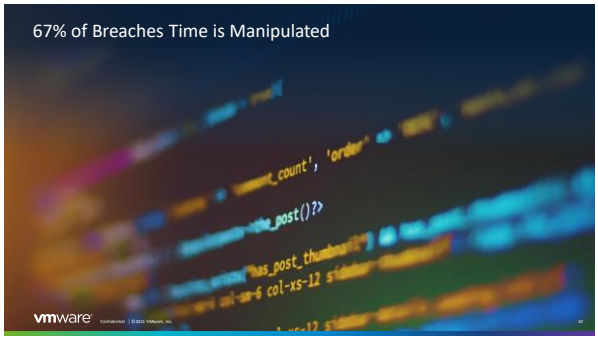
7


The Year of the Zeroday: Employed in 51% of Attacks
vmware

8


Counter Incident Response Occurs 61% of the Time
vmware

9


67% of Breaches Time is Manipulated
vmware

10


60% Experienced Island Hopping
The heist escalates to a hostage situation
vmware

11


RUSSIAN MARKET
vmware

12

13

Types of Destructive Attacks

I. Pure wipers
II. Denial of service
III. Repurposing of ransomware for use as wipers
IV. Deleting critical data and backups
V. Hybrid Attack: ICS manipulation

vmware Confidential | ©2021 VMware, Inc.

14

HermeticWiper aka DiskKILL

Wiper

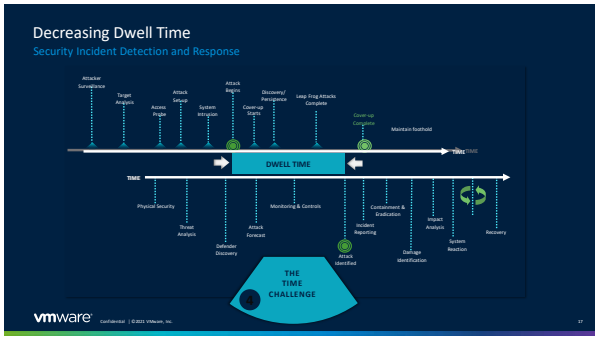
I. This malware leverages legitimate EaseUS Partition Master drivers to access the disk which in turn targets the Master Boot Record (MBR) of the disk.
II. During execution, the attacker targets privilege escalation before targeting the Domain Controller. The attacker will utilize Active Directory to move laterally to deploy.
III. It then corrupts the system's master boot record, displays a fake ransomware note.
IV. It erases "only" the first 100 hard drive available on the target system.

vmware Confidential | ©2021 VMware, Inc.

15


Offense Must Inform Defense
vmware
Confidential | ©2021 VMware, Inc.

16


Decreasing Dwell Time
Security Incident Detection and Response
Attacker Surveillance
Target Analysis
Access Probe
Attack Setup
System Intrusion
Attack Begins
Cover-up Starts
Discovery/ Persistence
Leap Frog Attacks Complete
Cover-up Complete
Maintain foothold
TIME
DWELL TIME
Physical Security
Threat Analysis
Defender Discovery
Attack Forecast
Monitoring & Controls
Attack Identified
Incident Reporting
Containment & Eradication
Damage Identification
Impact Analysis
System Reaction
Recovery
THE TIME CHALLENGE
vmware
Confidential | ©2021 VMware, Inc.

17


Threat Hunting Best Practices
Learn how to fight back
When discussing an intrusion, set up secure communication channels
Assume the adversary has multiple avenues back into the organization
To combat alert fatigue, baseline your organization
Build the capacity to detect and respond across workloads
Segment personal and professional networks
vmware
Confidential | ©2021 VMware, Inc.

18

2022 Security Strategy

Security solutions that interconnect, leveraging the infrastructure to address these issues:

Situational Awareness
Authoritative context of your environment and threat intelligence that is trustworthy, actionable and readily available

Connected Control Points
Workload, network, device and access controls and teams that connect and align to the applications and data being protected

Security as a Distributed Service
Minimize the number of agents and choke points and deliver security that follows the assets being protected - no matter what type of environment

19

19

Cybersafety for Colorado Schools

1. Validate that all remote access requires multi-factor authentication
2. Apply just in time administration
3. Disable all ports and protocols that are not essential for business purpose
4. Automate vulnerability management
5. Apply microsegmentation-- especially between student laptops and administration devices
6. Deploy Nextgen AV with EDR on all endpoints.
7. Deploy Workload security for a multi-cloud environment
9. Hire a Managed Detection and Response (MDR) firm
10. Utilize immutable backups

vmware Confidential | ©2021 VMware, Inc. 20

20

Personal Cyber Self-Defense

1. Update your operating system & apps
2. Turn your firewall on
3. Deploy Next-Gen Antivirus
4. Use a VPN
5. Turn your routers network security on.
6. Dedicate one router network for only work and finances

1. Use a sentence for your password
2. Always Turn MFA on.
3. Only you have admin rights
4. Use Signal for sensitive texts

vmware Confidential | ©2021 VMware, Inc.

21

Personal Cyber Self-Defense Cont.

11. Do ***not*** use public WIFI.
12. Use electric tape to cover cameras
13. Never use your debit card online.
14. Never click on links Remember the R2 rule
15. Your devices should lock after 5 min of non-use.
16. Delete your browser history every day.
17. Backup your data to a USB daily.
18. If you are hit by malware realize that you will have to change all your passwords across all of your accounts.
19. Finally do not leave Bluetooth on or location services on.
20. Limit Siri and Alexa's proximity settings.

22

Thank You

@TAKellermann

23