POINT OF VIEW

Cybersecurity and the Big Data Problem:

Human Security Operations Alone Struggle to Keep Pace

Executive Summary

Many of today's cyberattacks are broken into multiple stages of activity, each of which on its own is often difficult to discern as malicious rather than benign. Discernment is even more difficult given the volume of legitimate activity within which it naturally occurs given the diversity of work styles, devices, networks, applications, and cloud-delivery locations.

Simply put, effective human security analysis is exceptionally hard given the requirement to look through huge amounts of data for increasingly ambiguous signs of attack that only become more clearly malicious when viewed together as a complete multi-stage campaign. Imagine trying to piece together a puzzle when the pieces are not only small with muted colors but also mixed together with pieces of other puzzles. That's the task facing security analysts today.

Most cybercriminal techniques "abuse legitimate system tools … underscoring the idea that adversaries are attempting to appear as legitimate users."[1]

Threat Detection Challenge

Today's cyberthreat campaigns in general, and ransomware in particular, are increasingly sophisticated—sophisticated in regard to the number of coordinated stages that comprise a campaign as well as the ability of each stage to leverage activity that is also common within the operation of today's digital organizations.

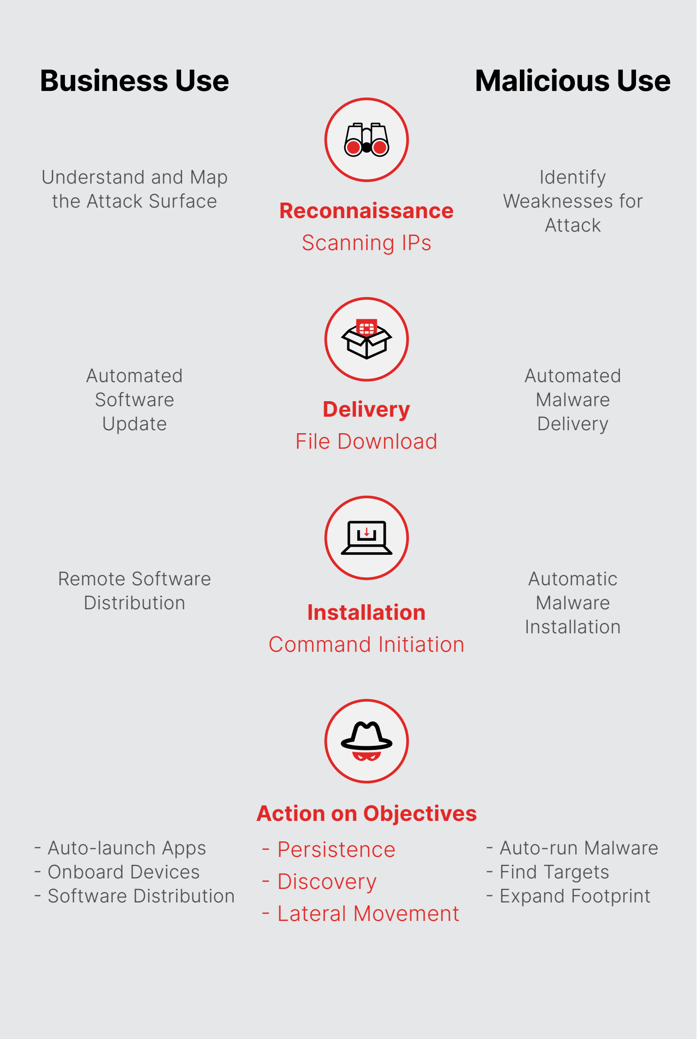
As a result, once past the traditional, prevention-oriented lines of defense, these campaigns can remain hidden and progress through to their ultimate outcomes, with impact increasing over an extended period of time—especially when they are mixed in among the huge volume and diversity of activity associated with today's digital organizations. Even with an experienced security team—dedicated to security monitoring, threat hunting, and incident response (which many organizations lack)—it is challenging for human operators to recognize, retain, connect, and understand each of these activities.

The Ambiguity of Attack Stages

FortiGuard Labs collaborated with the MITRE Center for Threat Informed Defense (CTID) to analyze more than 6 million techniques utilized across cybercampaigns over a two-year period and found that "15 techniques made up 90% [of the total observed]."[2] More importantly, "most of the these [15] techniques abuse legitimate system tools ... underscoring the idea that adversaries are attempting to appear as legitimate users."[3]

To highlight this challenge of separating malicious from legitimate activity, consider a common campaign flow, utilizing techniques that mirror normal operation.

- **Reconnaissance: scanning external IPs.** A common technique used by security teams to map the organization's external attack surface, it also provides cybercriminals with insight into avenues of attack.
- **Delivery: file download.** Routinely used for auto-updates, as well as user-initiated optimization (think browser plugins), such downloads can be compromised by cybercriminals as in the case of the side-loading Microsoft Defender update used as part of the Kaseya compromise.
- **Installation: command initiation.** Regularly utilized to push out software by IT teams, powershell is also a key method of executing malicious code without end-user action.
- **Command and Control.** While communications to external IP addresses may seem like an easy tell, it's actually quite often used by applications configured to communicate with cloud storage.



Business Use		Malicious Use
Understand and Map the Attack Surface	**Reconnaissance** Scanning IPs	Identify Weaknesses for Attack
Automated Software Update	**Delivery** File Download	Automated Malware Delivery
Remote Software Distribution	**Installation** Command Initiation	Automatic Malware Installation
- Auto-launch Apps - Onboard Devices - Software Distribution	**Action on Objectives** - Persistence - Discovery - Lateral Movement	- Auto-run Malware - Find Targets - Expand Footprint

- **Action on Objective: persistence.** Convenient for end users, common applications are scheduled to auto-run at start, which also allows malware to remain in operations on a system over time.
- **Action on Objective: discovery.** Also used by preconfigured applications, discovery of devices, databases, and other IT infrastructure, discovery communications allow cybercriminals to map the organization.
- **Action on Objective: lateral movement.** PSExec, an established tool for system administrators, is also a key method for cybercriminals and components to move laterally to high-value targets.

Going one step further, as we look at the 15 most common techniques noted earlier, more than half of them—command and scripting interpreter, signed binary, WMI, remote services, scheduled task, modify registry, modify process, ingress tool transfer, proxy—routinely occur each week. And even the remaining actions—hijack execution flow, process injection, non-application layer protocol, masquerading, impair defenses, obfuscated files—are specifically designed to hide themselves.

So while these are common cybercriminal stages and techniques, used by cybercampaigns like Emotet, Ryuk, and other ransomware as catalogued by MITRE within its ATT&CK framework and tested during ATT&CK evaluations, they also regularly occur as normal operational activity.

The Volume of Activity and Event Information

Not only that, consider the magnitude of security information being collected from across the organization. In the fourth quarter of 2021, every minute of every day, Fortinet products protected against:

- 28 million network intrusion attempts (up 432% from 4Q20)
- 124 thousand phishing attempts (down 9%)
- 555 thousand malicious website access attempts (up 20%)
- 3.5 million malware programs (up 283%)
- 41 million command and control attempts (up 175%)

And that's just malicious cyberactivity. There is a correspondingly high volume of legitimate activity occurring as well.

According to SolarWinds, the average employee endpoint generates five events per second; each network switch logs 150 events per second; Windows domain server generates 35 events per second; and servers generate 3–4 events per second. At the same time, the external firewall generates 60 events per second; IPS generates 70 events per second; and the antispam gateway generates five events per second[4]... making it even more difficult to see, let alone analyze, potential incident indicators.

Conclusion

Even the most expert security analysts face an often insurmountable task of identifying multi-stage cybercampaigns, designed to mimic the activity of legitimate users and systems, within the volume and diversity of normal activity of today's digital organizations. It is no wonder that cyberthreats like ransomware are arguably more successful than ever, through no fault of security pros.

[1] "Sightings Ecosystem: A Data-Driven Analysis of ATT&CK in the Wild," MITRE Engenuity CTID, 2021.

[2] Ibid.

[3] Ibid.

[4] Brad Hale, "Estimating Log Generation for Security Information Event and Log Management," SolarWinds.

FORTINET

www.fortinet.com

Copyright © 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

April 1, 2022 7:05 AM
1541364-0-0-EN