SOLUTION BRIEF

Thwart Ransomware With Artificial Intelligence Across the Cyber Kill Chain

Today's Ransomware Risk

Today's ransomware is often specifically engineered to bypass traditional, prevention-oriented security controls by distributing campaigns across multiple stages, each increasingly engineered to leverage legitimate applications, communications, and other activities to blend in with normal operations. This sophistication makes it exceptionally difficult for even seasoned security staff to detect attacks in progress amid the high volume of daily activity and event information and respond fast enough to prevent encryption of systems.

Ransomware payments in 2021 topped those of the past decade.

In addition to the financial cost of ransom payouts—which, in 2021, the U.S. Treasury estimated topped those of the entire past decade—ransomware has interrupted healthcare, manufacturing, transportation, and other critical business operations. Without question, the ability to detect and interrupt ransomware before it interrupts operations is essential.

Detect Ransomware Across the Cyber Kill Chain

The good news is that Fortinet offers a range of advanced threat detection products to identify ransomware campaigns at each stage of the cyber kill chain, using the multi-stage sophistication of such campaigns against the cybercriminal. Specifically, many of the products leverage artificial intelligence (AI), machine learning (ML), and deep learning (DL), along with other advanced analytics to:

- Process the huge volume of event data generated by today's digital organizations
- Identify anomalous and high-risk activity that often mimics legitimate operations
- Cover the entire attack surface and cyber kill chain stages to stitch together a comprehensive picture
- Integrate with traditional security controls within a cybersecurity platform to simplify and speed operations

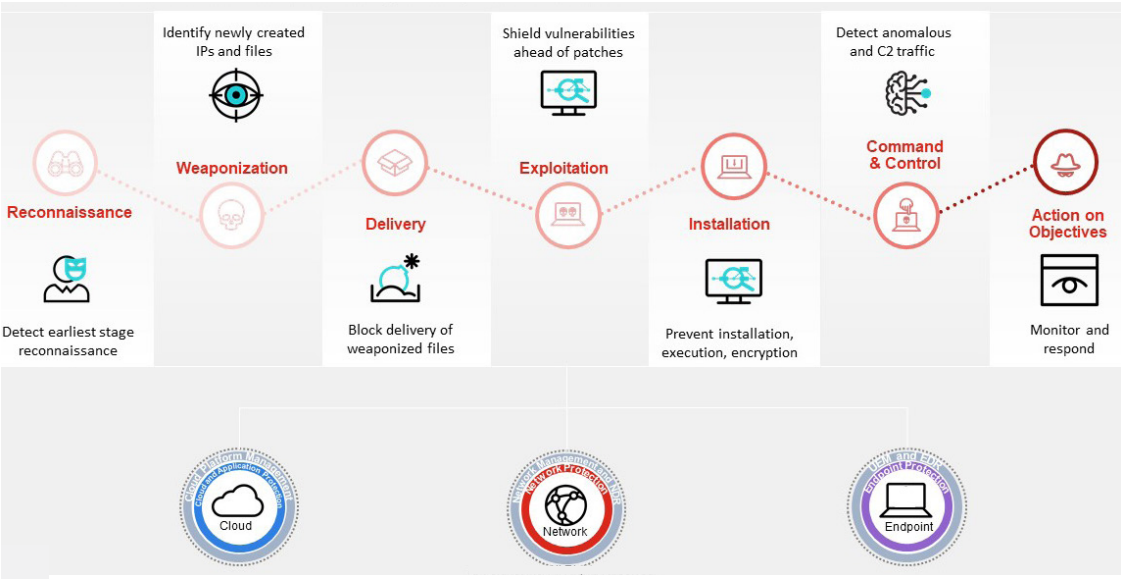

Figure 1: Integrated, AI-powered prevention and detection along the cyber kill chain

Reconnaissance

FortiDeceptor enables organizations to deploy a range of decoys and lures that accurately replicate common, high-value infrastructure attractive to cybercriminals. These can be internet-accessible and flag early-stage reconnaissance that precedes actual cyberattacks. It can also identify internal network discovery and attempted lateral movement, in all cases working with the firewall to automatically block communications to and from malicious or compromised IP addresses.

Weaponization

FortiRecon automatically identifies an organization's attack surface and can proactively uncover external infrastructure and objects that cybercriminals may have prepared before a cyberattack.

Delivery

FortiSandbox includes multiple ML engines to provide static analysis of code in transit and the dynamic analysis of code running in a secure, instrumented environment. Further, the Virtual Security Analyst of FortiNDR utilizes an artificial neural network to provide sub-second detection of previously unknown malware, including insight into its feature makeup against more than two dozen common threat classes. Both products can integrate across multiple attack vectors to identify code seeking entry via email, the web, various cloud applications, and more and automate the corresponding response actions.

Exploitation, Installation, and Execution

FortiEDR identifies vulnerable applications and shields them from exploit while an ML engine blocks the installation of malicious code without the need for pre-existing threat intelligence. Behavior analytics, both on the device (for patented detect and defuse of running code) and a dynamic control flow engine in the cloud, continue classifying and reclassifying system activity. A predefined response framework automates the containment and remediation function.

Command & Control

FortiNDR utilizes an ML engine to profile network activity and identify deviations (including new outbound communications), along with a series of pragmatic analytics to identify additional indicators of risk, such as weak ciphers, vulnerable protocols, and IoCs related to ongoing cybercampaigns. Again, integrations with the firewall as well as security orchestration, automation, and response platforms speed investigation and containment.

Action on Objectives

Many of the above products can identify the action on objectives of cybercriminals, including compromised devices, lateral movement, data exfiltration, data encryption, and more.

Speed Response Through Integration and Automation

As a result, organizations that deploy one or more Fortinet breach protection portfolio components will improve their organization's mean time to detect ransomware and other cyberattacks with the aid of various AI engines. This faster detection will certainly speed mean time to response (MTTR) on its own. But the integration of these components with the security controls distributed across the attack surface accelerates MTTR even further through automation.

Needless to say, detecting ransomware faster—in many cases at cyber kill chain stages that precede the data destruction/encryption function—greatly reduces the risk of downtime. Depending on the organization, that may mean more lives saved (in the instance of healthcare or critical infrastructure) or more profitability (in manufacturing, biotechnology, food processing, financial services, and others).

Further, automation also improves the efficiency of security operations, productivity of security teams, and overall productivity.

Conclusion

Fortinet Breach Protection products can be deployed to reduce ransomware at multiple stages of the cyber kill chain, wherever the organization sees a gap or weakness. Further, they can operate as integrated extensions of distributed security controls to cover the broad attack surface and automate response. Of course, products must be complemented by preparation, practice, and perpetual monitoring, which are also available as part of, or augmentation to, the Fortinet Security Fabric.

Organizations moving toward a cybersecurity mesh architecture should take full advantage of the Fortinet Security Fabric over time for consolidation and effective, efficient security. The Fortinet Security Fabric exemplifies this concept by:

- Applying AI and advanced analytics for risk-based scoring and detection of sophisticated threats
- Reducing complexity through robust APIs and integration within a cybersecurity platform to speed response
- Extending security controls deployed across the broad attack surface

Solutions

FortiDeceptor

FortiRecon

FortiSandbox

FortiEDR

FortiNDR

www.fortinet.com

March 19, 2022 4:56 AM
1507986-0-0-EN