NYOTRON
SECURING THE WORLD

NYOTRON THREAT BRIEF

Make Your Threat-Agnostic Defense™ PARANOID. So You Don't Have to Be.

Nyotron Threat Brief
COPING WITH RANSOMWARE

BACKGROUND

Recently, enterprises have been experiencing CryptoLocker / Ransomware attacks. These enterprises are heavily armed with security products and advanced policies, but still stay exposed to new and changing forms of threats, such as encrypting ransomware. The attackers use social engineering techniques to persuade an employee to run their executables as they seem legitimate and harmless, but in fact, they encrypt data files and subsequently demand a ransom for retrieving their decryption key.

Advanced encrypting ransomware, such as TeslaCrypt, CHIMERA, and the very latest PETYA and PowerWare Fileless Ransomware, are targeting enterprises and causing severe damage. The damage results in major loss of data together with a potential complete shutdown of critical services.

Usually, these attacks bypass the security barriers because there are thousands of samples for each attack campaign. The antivirus databases cannot possibly be up-to-date with all the variations in such a short time between ransomware deployment and attacks.

The encrypting ransomware behaves differently for each attack campaign: some call back to proxy servers while others inject themselves into other processes. with the emergence of Chimera ransomware, the victims are also prone to major data leaks as the ransomware developers threaten to put the corporate files into the public domain if the ransom amount is not paid by the deadline.

The latest PETYA attack encrypts the computer disk MFT, blocking any access to its files. Other PETYA versions are designed to spread and hit servers. What's next with these types of threats? We cannot expect clear or accurate predictions. This is why a new security paradigm was developed in order to generically prevent any future threats, without actually having to know anything about the threat.

PARANOID DISRUPTIVE PARADIGM VS. DATA CORRUPTION ATTACKS

Nyotron's industry-changing solution was designed to prevent unprecedented types of targeted, highly advanced and national-level cyber attacks, as well as mitigate threats that are already inside the enterprise. PARANOID is focused on the damage phase of an attack with our patented Behavioral Pattern Map (BPM) technology. The BPM engine simply maps a computer's operating system to represent all normative OS patterns that execute any computer activity that may

NYOTRON
SECURING THE WORLD

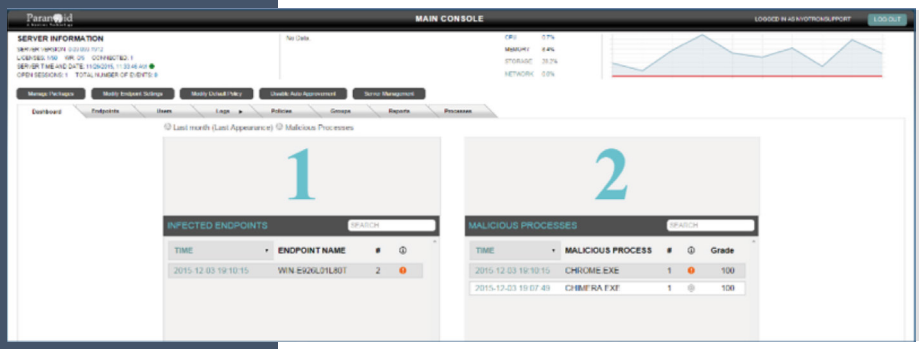
2880 Lakeside Drive
Suite 237
Santa Clara, CA 95054
+1.408.780.0750
www.nyotron.com

become dangerous. Ultimately, PARANOID is immediately able to identify “bad” OS patterns and prevent malicious activity, before it can reach its goal - causing damage, such as file deletion or malicious encryption damage.

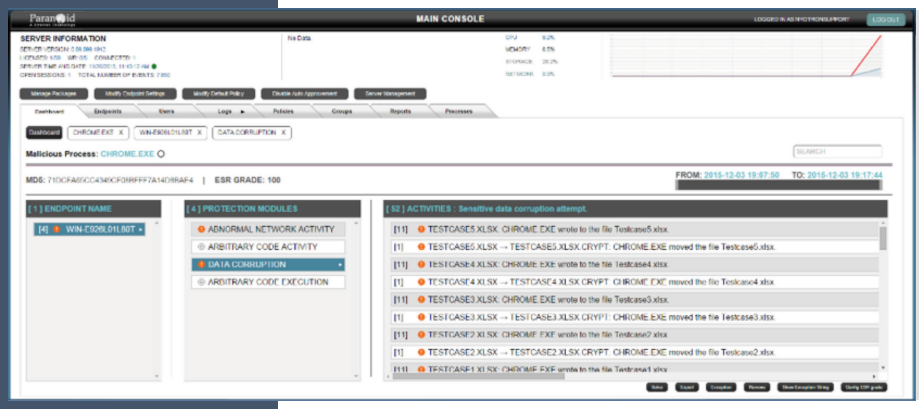
Based on a damage-driven mechanism, PARANOID alerts on activities during the attack setup phase, such as process injections and registry manipulations. It also prevents activities on the attack objectives such as data exfiltration and data destruction/encryption (see the screenshot in step 2 below).

A REAL-LIFE EXAMPLE: FINANCIAL INSTITUTE

The screenshots below represent a proof of concept process conducted by the cyber department of a large financial institution. Challenged with a dozen different Ransomware variations, PARANOID proved to detect and prevent 100% of them, with no special policy setup or product enhancement.



Step 1
As CryptoLocker executes:
The PARANOID console shows the main malicious process and its injected process on the main dashboard.



Step 2
Drill down in to the attack:
PARANOID tracks, logs and eventually blocks the attack flow before any damage is caused to the files.

CONCLUSION

PARANOID’s Behavioral Pattern Mapping technology was developed long before PETYA or TeslaCrypt appeared in the market, and still successfully deals with them – in the same manner that it will deal with the next type of ransomware or other upcoming threat family which is being currently being developed.

Delivering the first ever threat-agnostic technology, the PARANOID differentiator is clear - PARANOID is effective immediately for existing inside threats, or upcoming threats without the need to learn how the threat actual structure or details, their nature, their attack vectors, threat origin, or any other of the “machine learning” or mathematical-based security methods.

NYOTRON
SECURING THE WORLD

2880 Lakeside Drive
Suite 237
Santa Clara, CA 95054
+1.408.780.0750
www.nyotron.com