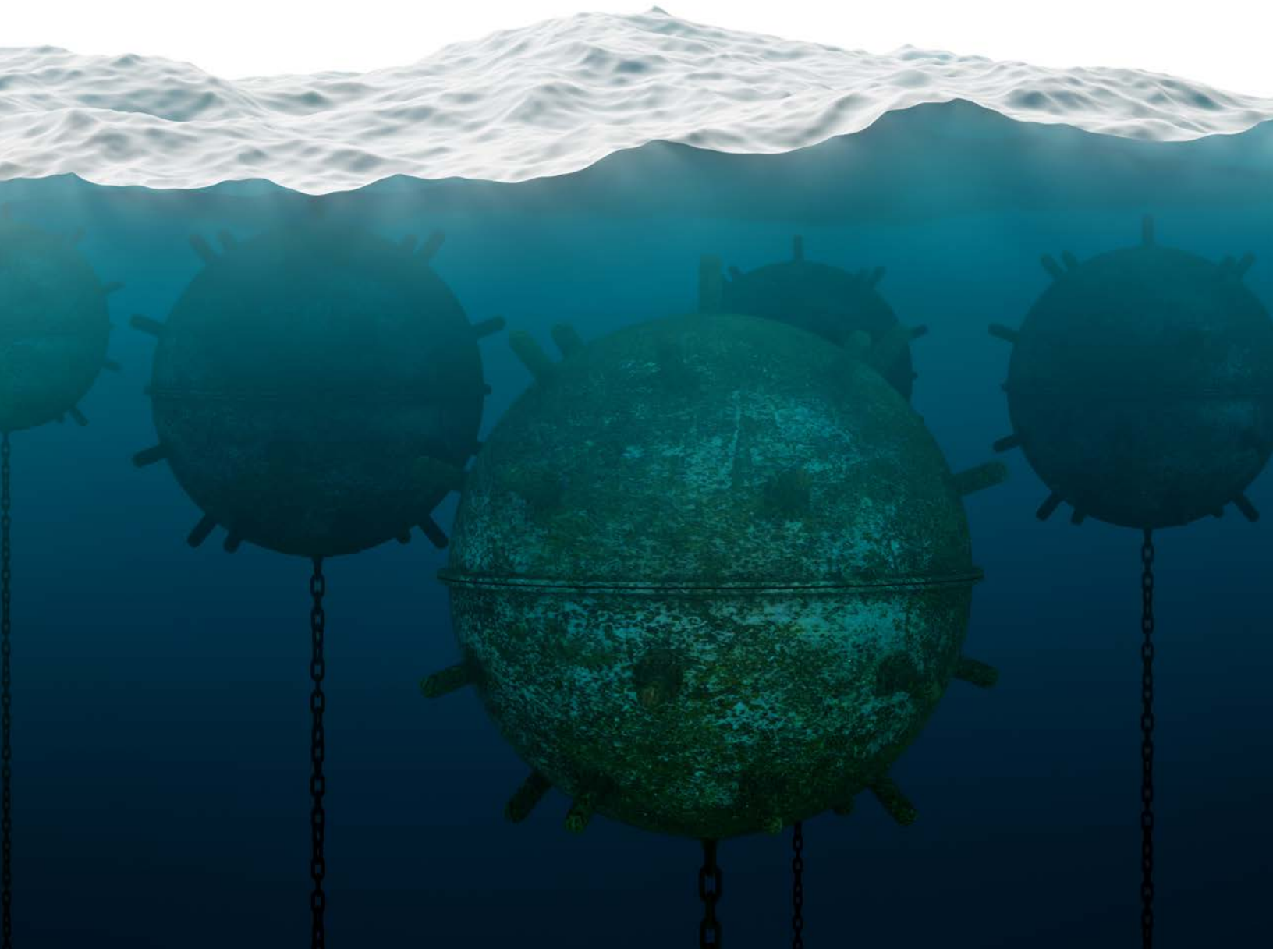
Protecting the Enterprise Against Unknown Malware

What you can't see can hurt you. Why Threat hunting is an essential tool to combat the rise of unknown malware.



WHITE PAPER

Infocyte®

Table of Contents

Executive Summary

Last year stands out for the astronomical growth of malware, resulting in a significant increase in the sheer volume of cyberattacks on enterprises, organizations, nations and infrastructure.

Some estimate that in 2016 malware attacks quadrupled from previous numbers. It was a year marked by extraordinary attacks, including multi-million dollar virtual bank heists and overt attempts by state-sponsored groups to disrupt the democratic electoral process in many Western countries.

2016 marked a massive jump in the volume of unknown malware being created and downloaded, with a 900% increase and more than 970 downloads per hour - compared with 106 previously.[1]

Cyber criminals caused unprecedented levels of disruption with relatively simple IT tools and cloud services. In 2016, researchers at CheckPoint painted a dire picture of an average day in the life of a typical enterprise1:

- Every 81 seconds a known malware is downloaded
- Every 4 minutes a high-risk application is used
- Every 4 seconds an unknown malware is downloaded
- Every 5 seconds a host accesses a malicious website
- Every 53 seconds a bot communicates with its command and control center
- Every 30 seconds a threat emulation occurs

The research also indicated a massive jump in the volume of unknown malware being created and downloaded: a 900% increase, with more than 970 downloads per hour - compared with 106 previously. More than 12 million new malware variants were released each month.

The rate at which new malware is being developed has soared - data shows that more new malware has been developed in the past few years than in the previous 10 years combined. Malware is being developed at such a rate that traditional anti-virus and anti-malware software solutions are struggling to keep up.

This white paper introduces threat hunting as an essential component of your security strategy to combat the rise of unknown malware. We will examine the increased threats for 2017 and provide guidance on how to respond and react to malware using threat hunting.

[1] CheckPoint Security Report, 2016

Impact of Cyberattacks

There is no dispute, the proliferation of malware and cyberattacks is at an all-time high, and forecast to continue to increase. There are many ways that malware is used to attack enterprises and organizations - however fileless malware and other advanced persistent threats such as botnets, rootkits, RATs, macro enabled documents and scripts are arguably the most dangerous. These threats bypass security defenses, usually remain undetected for long periods of time, and are difficult to track even once the problem has surfaced.

Overall economic cybercrime has evolved to a point where one can segment it into two distinct categories — the kind that steal money or data that is monetizable and bruise reputations; and the kind that steal IP and lay waste to an entire business. The latter are often classified as 'transfer of wealth' attacks.

While the long-term damage, both to organizations and the economy, is potentially far higher for transfer of wealth attacks - the regulatory pain, loss of investor confidence and media scrutiny arising from the theft of funds, medical data, financial details or of personally identifiable information can be damaging too. As regulation and oversight catches up, organizations will increasingly find themselves having to deal with legal implications in the event of an incident occurring.

The Evolution of Attackers and the Malware Used

Recent years have seen a proliferation of both malware and the hostile actors that use malicious software for illegal monetary gain, to obtain proprietary or sensitive information, to influence society and electoral processes or to encourage general instability.

Attackers typically fall into one of five categories:

Nation-states: threats include espionage and cyber warfare; victims include government agencies, infrastructure, energy and IP-rich organizations

Insiders: not only your employees but also trusted third parties with access to sensitive data who are not directly under your control

Terrorists: still a relatively nascent threat, threats include disruption and cyber warfare; victims include government agencies, infrastructure and energy

Organized crime syndicates: threats include theft of financial or personally identifiable information (sometimes with the collusion of insiders); victims include financial institutions, retailers, medical and hospitality companies

Hacktivists: threats include service disruptions or reputational damage; victims include high-profile organizations and governments; victims can include any kind of organization

Organizations and enterprises have been struck in attacks leading to high profile breaches by: Lazarus Group, APT28, and nation-backed groups such as Helix Kitten and Fancy Bear.

From banks and financial institutions to media infrastructure, political parties and nation states - no segment of society has been immune from attack.

NOTABLE NEW AND RECYCLED MALWARE

- **NotPetya** - cyberattack that masqueraded as ransomware, targeting critical infrastructure. Exploited vulnerabilities in Windows, encrypting files and destroying recovery keys.
- **Fireball -** infected 250 million computers worldwide. Adware that had the ability to run any malicious code, direct users to malicious websites, drop malware and spy. Design included evasion and mutli-layer anti-detection techniques.
- **WannaCry** - massive ransomware attack with worm capabilities. This cyberattack used intelligence community techniques leaked by the Shadow Brokers.
- **Kovter** - a sophisticated form of malware that can invade a user's system by creating a registry key instead of downloading a file. Kovter is also able to identify and deactivate security programs that are designed to root it out
- **EternalBlue, EmeraldThread and Eternal Champion** - exploits targeting Microsoft systems released by Shadow Brokers
- **Longhorn** - malware with detailed system fingerprinting, discovery, and exfiltration capabilities. The malware uses a high degree of operational security, communicating externally at only select times, with upload limits on exfiltrated data, and randomization of communication intervals
- **Old fashioned infection techniques** such as VBA Macros and a flurry of scripting languages (JavaScript, VBScript, etc) returned.
- **Lazarus code** seen in new forms used in heist of $81 M from Central Bank of Bangladesh

New Hacking Tools Leaked

In a sign of the times, this year began with a proliferation of intelligence community tools made widely available on the internet. Wikileaks released 'Vault 7' CIA hacking tools from its malware arsenal including dozens of zero day weaponized exploits.

Similarly, the Shadow Brokers released what were claimed to be NSA attack tools, and Russian and Chinese “cyber-communities” immediately began actively researching and sharing information on the tools, indicating that cyber-criminals and state hackers would be looking to capitalize on unpatched systems around the world. In mid May 2017, this very event occurred on a massive scale. Aptly dubbed 'Wannacry', this event crippled tens of thousands of computers worldwide in what is one of the largest single cyberattack to date. Hospitals, educational institutions, communications infrastructure, logistics and government entities were targeted.

Wannacry was closely followed by the NotPetya attack, which used the same EternalBlue exploit to infect computers on local networks. However unlike Wannacry, which was true ransomware, NotPetya was in fact a wiper that rendered files permanently encrypted.

Estimates for the annual economic costs of global cybercrime pinpoint a figure of $450 billion USD. Last year, over 2 billion personal records were stolen and in the U.S. alone, over 100 million people had their medical records stolen.

Estimates for the annual economic costs of global cybercrime pinpoint a figure of $450 billion USD. Last year, over 2 billion personal records were stolen and in the U.S. alone, over 100 million people had their medical records stolen.

While this has led to big business for insurance companies, the level of unpreparedness is worrying. A report released earlier this year by specialist insurer Hiscox found that across businesses in U.K., U.S. and Germany - 53% of the organizations were ill prepared to deal with an attack.

Forecast for the balance of 2017

Malware attacks will continue and spread. Ransomware will continue to plague individuals and companies, but be prepared also for more sophisticated phishing techniques and an increase in the deployment of exploit kits that have enhanced capabilities for evading detection.

Critical infrastructure will become a greater target - most of the world's infrastructure was designed and built before the threat of cyberattacks. As such, most of it has virtually no electronic information security measures in place. Such targets will be impossible to resist for malicious actors.

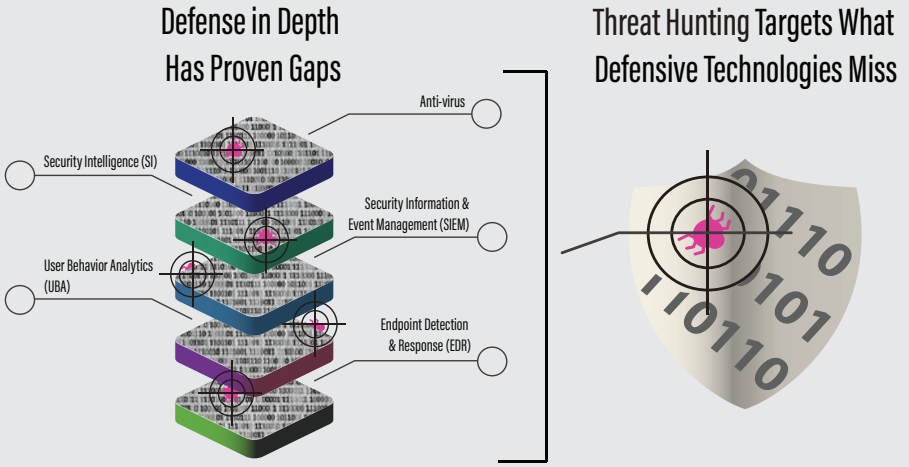
National security will come under increased threat from cyberattacks, as state sponsored actors continue to target democratic election processes, both directly through attacks on political parties, organizations and candidates - and indirectly through attacks on media and third party entities associated with political parties such as think tanks.

It's important for enterprises to understand the threat landscape and the present realities that govern security today. The fact is, malware attacks will continue and increase in frequency.

The reason such attacks commonly result in high profile data leaks or loss of funds, is because defensive solutions simply do not and can not protect enterprises from all threats. Some threats will breach defenses. To make matters worse, the average security breach goes undetected for over six months. This problem is known as the breach detection gap, or dwell time, and is one of the greatest threats to the security of an organizations systems and data.

The approach many organizations take is to simply layer on increasing numbers of defensive solutions.

Defense is important, but is not the only factor to deliver security. Threat Hunting is necessary in order to catch what defensive technologies miss.



Mitigate Your Risk: How to Respond and React to Malware

The Ponemon Institute's 2017 Cost of Data Breach Study: Global Overview found that how quickly an organization contained a data breach, had a direct effect on the financial impact. Case in point, the cost of a data breach was nearly $1 million lower for organizations that were able to contain the breach in less than thirty days. To achieve any sense of legitimate security, enterprises must instill a protocol to define and manage dwell time.

The key steps that anchor this process are:

- Organizations need to determine an acceptable "breach discovery window" for threats that have slipped through existing defenses; then
- They must enforce it by proactively hunting for malware that has breached in order to discover it within the established time frame.

The following 4 key principles are helpful in navigating this process:

1. Accept that malware and APTs will breach existing defenses; and
2. Endpoints should be treated as untrusted until proven otherwise; and
3. Any trust established is both finite and fleeting; and
4. Endpoints need to be validated as malware free – anytime, anyplace.

The simplest way for enterprises to adhere to these principles, is to put a threat hunting solution in place that can root out threats that have breached defenses and are persisting undetected – and use it to enforce the breach discovery window.

Expose Unknown Malware with Infocyte HUNT™

Hunting for malware and persistent threats is usually an activity that requires teams of highly skilled forensic experts to acquire memory dumps and analyze the raw data using techniques such as volatile memory analysis. Lacking access to such specialized resources, the approach many organizations take is to simply layer on increasing numbers of defensive solutions.

Defense is important, but it is not the only factor to deliver security.

Infocyte approaches threat detection from a completely new perspective - by presuming endpoints are already compromised. Infocyte HUNT is designed to rapidly assess endpoints for evidence of compromise, even the most elusive rootkits and backdoors.

Infocyte HUNT combines forensic automation and volatile memory analysis techniques to detect malware, suspicious code and persistent threats that have breached existing defenses. The platform does not rely on host OS for data, which may itself be compromised.

Users of Infocyte HUNT are able to define and manage the breach detection gap - the period of time between infection and discovery. Enterprises can determine exactly how long they are willing to tolerate unknown threats within their organization.

Infocyte HUNT offers organizations the ability to scan, find, and identify any suspicious software that has penetrated defenses – whether the malware is known or unknown, active or dormant.

Start Hunting. Contact Us.

[2] 2017 Cost of Data Breach Study: Global Overview

About Infocyte

Developed by former US Air Force cybersecurity officers, Infocyte's hunt technology fills a void left by today's real-time detection solutions. By focusing on the post-compromise activity of persistent attackers and insider threats, Infocyte's unique approach to security helps organizations defend their networks and critical information.

CORPORATE HEADQUARTERS

110 E. Houston St. Floor 6

San Antonio, TX 78205

+ 1.844.INFOCYTE (844.463.6298)

sales@infocyte.com

www.infocyte.com

@InfocyteInc