FORTRA™

After WannaCry – Getting Ahead of Ransomware

Protecting Your Organization From Ransomware

Table of Contents

PART ONE

WannaCry 101

What is WannaCry Ransomware

The WannaCry ransomware is one of largest and worst ransomware campaigns ever, spreading to over 200,000 computers spanning 150 countries in the course of a weekend. The attack began with UK's National Health Services(NHS) and spread all over the world to several businesses including Telefonica and several other large companies in Spain, as well as FedEx, Deutsche Bahn, and LATAM Airlines.

Upon infection, WannaCry displayed a ransom screen informing the victim that their files have been encrypted and demanded a payment in bitcoin, typically equivalent to $300, within three days. If the user did nothing after 3 days, the ransom doubled.

How WannaCry Became An Outbreak

The WannaCry attack that started on Friday, 12 May 2017 is different in a lot of ways. The malware selfpropagated like a worm unlike other ransomware variants that rely on phishing emails. It look place in steps:

1. The attack targeted Windows machines with specific vulnerable version of SMB ports exposed to the internet.

2. It then used an exploit called ExternalBlue to install a backdoor that worked over the internet without requiring any user interaction.

3. Once the malware 'WannaCry' was installed on a targeted system the ransomware encrypted files that were stored on the machine.

4. The malware began to spread laterally.

"It's not just encrypting files and locking users out of their machines, but it's also self-propagating and uses exploit code, behavior that hasn't been seen in ransomware until now. WannaCry behaves a lot like the Internet worms that were common about 10 or 15 years ago. Once it's on a new machine, the ransomware will scan the network the computer is on, looking for any other PCs with the SMB vulnerability and port 445 open. If it identifies a vulnerable machine, it then delivers the EternalBlue exploit and starts the cycle all over again."

- DENNIS FISHER
EDITOR-IN-CHIEF OF ON THE WIRE

PART TWO

Experts on How To Get Ahead of Ransomware

Bulletproof Your Backup and Recovery Practices

“SOMETIMES IT MAY SEEM EASIER TO JUST PAY THE RANSOM, BUT WHY NOT MITIGATE THE THREAT IN THE FIRST PLACE? WITH PROPER BACKUPS IN PLACE, YOU CAN VIRTUALLY ELIMINATE AN ATTACKER'S ABILITY TO BLACKMAIL.”

- Focus on frequent and clean backups
- Schedule frequent backups
- Watch backups for malware

Free Download

Download the Forrester Report on "Ransomware Protection Best Practices"

(source: Ransomware Protection Best Practices" by Chris Sherman and John Kindervag, Forrester Research, November 4, 2016)

Protect Against Phishing And Watering Hole Attacks

"DON'T BLAME THE VICTIMS; INSTEAD, GIVE THEM THE RIGHT TOOLS."

- Leverage antispam, phishing, and web control tools for employee protection. Ensure proper protections are in place.
- Encourage the human firewall. Train staff in a manner that explains why you're doing the training; employees are more understanding and motivated if they get it.

Free Download

Download Infographics Don't Get HOOKED - How to Recognize and Avoid PHISHING ATTACKS

(source: Ransomware Protection Best Practices" by Chris Sherman and John Kindervag, Forrester Research, November 4, 2016)

IT Hygiene isn't Optional

"The WannaCry outbreak should reiterate the value of patching in a timely and efficient manner as soon as possible in order to avoid leaving the attack surface exposed for prolonged periods of time. In this case the patch was released by Microsoft for this critical yet non-zero-day vulnerability back on March 17, 2017, approximately 55 days prior to the manifestation of WannaCrypt in the wild."

- WILL GRAGIDO
DIRECTOR OF PRODUCT LINE
ADVANCED THREAT PRODUCTS AT DIGITAL GUARDIAN

Will Gragido is a seasoned security professional with over 20 years' experience in networking and information security. Will's extensive background is the result of his service as a United States Marine, a consultant with the world renowned International Network Services, Internet Security Systems (now IBM ISS), McAfee, Damballa, Cassandra Security, RSA Netwitness, Carbon Black, Digital Shadows and now Fortra™'s Digital Guardian® where he leads the organization's Advanced Threat Protection Product Line as its Director.

When Patching isn't an Option, Employ Compensating Controls

"Because we live in a world where code is developed and released often in what is considered a "vulnerable" state, organizations need to consider their use of compensating controls."

– WILL GRAGIDO
DIRECTOR OF PRODUCT LINE
ADVANCED THREAT PRODUCTS AT DIGITAL GUARDIAN

- Compensating controls at times are referred to as 'virtual patches' – a term originally coined by Internet Security Systems.
- These controls can be network or host resident technologies such as FW, NGFW, IPS (network or host).
- They mitigate risks posed by the threats who might exploit vulnerable systems which were being protected by said compensating control.

The Future of Ransomware

WannaCry is bad. But it's probably just a hint of what's coming. Researchers have been warning about the potential for a large-scale ransomware worm like this for some time, and while WannaCry has caused some trouble, it could be a lot worse. A ransomware worm that targets IoT or ICS systems would have the potential to truly wreak havoc on a massive scale. Imagine traffic lights or autonomous cars being held for ransom. It's not a pretty picture but it probably isn't too far off in the future either.

- DENNIS FISHER
EDITOR-IN-CHIEF
ON THE WIRE

PART THREE

How Digital Guardian Stopped WannaCry

How Digital Guardian Protected Customers From WannaCry

Upon hearing of the outbreak, Digital Guardian's Advanced Threat Team worked swiftly to update our Ransomware Content Pack and validated that the Digital Guardian agent can prevent the WannaCry ransomware from running.

Digital Guardian customers subscribed to our Managed Security Program for Advanced Threat Protection were automatically protected. On-premise customers of the Digital Guardian endpoint agent version 7.x received the updated Ransomware Content Pack for free.

We urge all customers to take this threat very seriously and implement measures to mitigate against potential infections capable of disrupting normal system operations, including patching software immediately, backing up data to an off-network location, and educating employees about the threat.

The incident response effort was led by Tim Bandos, our Senior Director of Cyber Security and a former Fortune 100 cyber security leader.

Free Download

Get the Incident Response Field Guide written by Tim Bandos. This eBook provides easy-to-follow steps for crafting an incident response plan in the event of cyber security attacks.

PART FOUR

Digital Guardian for Protection Against Ransomware

Traditional Signature-Based Antivirus Solutions Are Ineffective

Cybercriminals have turned to ransomware as the latest go-to tool for attacking and extorting businesses using a wide range of variants such as WannaCry, Cryptowall, Samas, Locky, and TeslaCrypt.

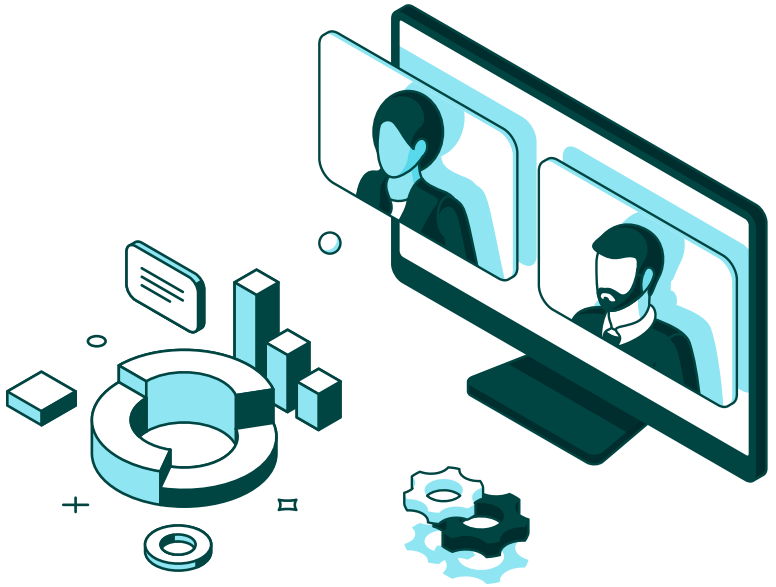
Traditional signature-based antivirus and threat detection methods have proven to be ineffective at protecting against ransomware attacks, which often employ new and evolving variants to evade detection. Digital Guardian's Managed Security Program for Advanced Threat Protection (ATP) provides the highest level of protection from ransomware attacks by focusing on understanding and protecting the attackers' main target - your data.

Digital Guardian Managed Security Program for Advanced Threat Protection

Detect And Prevent Ransomware in Real-Time

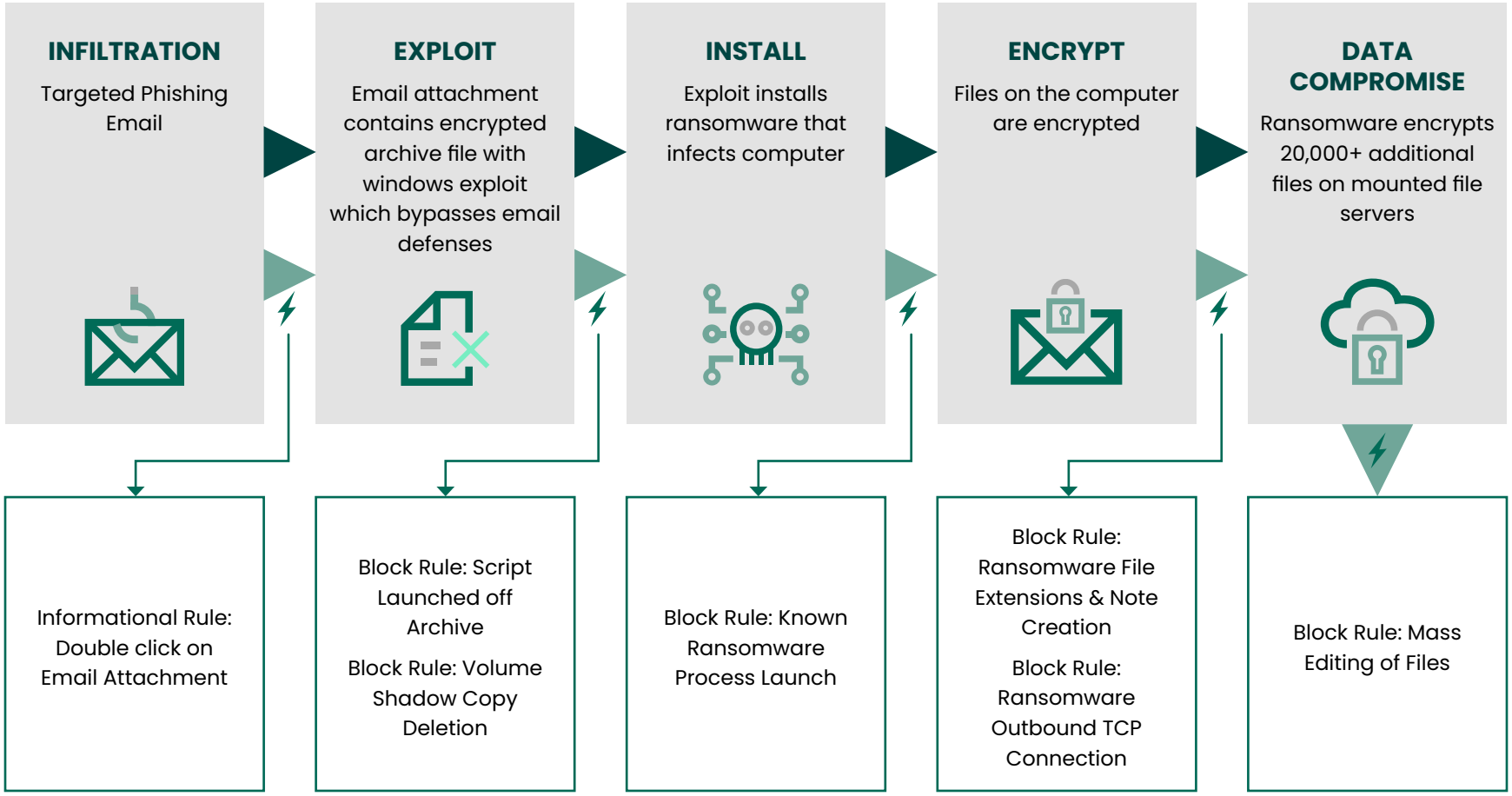
Our Advanced Threat Protection (ATP) solution uses a combination of threat intelligence and behavior-based detection to stop ransomware before it compromises your organization. Digital Guardian's ATP provides deepest visibility into infection sequence and detects behaviors indicative of ransomware.

Behavioral rules detect and block advanced threats across their entire lifecycle. The rules can even prevent the encryption routines from being applied to your most sensitive data and protect the data from being compromised.



Digital Guardian In Action

The chart below highlights each of the stages of an attack and the corresponding mitigative controls provided by Digital Guardian's Advanced Threat Protection.



PART FIVE

Advanced Threat Protection As A Service

When Does It Make Sense to Consider ATP as a Service?

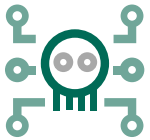
If any of these apply to your organization it may make sense to outsource or augment your Incident Response team with an Advanced Threat Protection Managed Security Program:

SECURITY TALENT SHORTAGE

The severe security talent shortage, especially for cyber security professionals, is preventing you from finding and retaining the people you need to build an IR team.

HEADCOUNT CHALLENGES

The political climate of your organization makes it difficult to gain approval for the 3-5 people you need to build an effective IR team.



COMPLEXITY OF STAYING ON TOP OF SOPHISTICATED MALWARE

Modern malware is sophisticated, targeted and difficult to detect. According to Verizon's latest Data Breach Investigations Report, companies on an average went more than 200 days between the time they were breached and the day they discovered the malware. As malwares get smarter, your ability to prevent the loss of sensitive data on your own gets harder and harder.

Advanced Threat Protection Managed Security Program

The Latest Defense Strategies And Intelligence

Our Advanced Threat Protection Managed Security Program is led by Tim Bandos, Director of Cybersecurity. The program combines security researchers and analysts' expertise, Digital Guardian's Next Generation Data Protection Platform and a centralized threat intelligence management system. This combination enables Digital Guardian to detect and remediate threats faster and more efficiently. You can expect the highest level of protection from threats including polymorphic malware, zero-day attacks, advanced persistent threats (APTs), ransomware and attacks involving sophisticated data theft methods.

Digital Guardian Managed Security Program for Advanced Threat Protection

Why Digital Guardian?

Real-Time Visibility

Digital Guardian's continuous endpoint monitoring includes real-time and historic visibility into more than 200+ parameters associated with system activities. Visibility into the entire kill chain lifecycle means more effective detection & analysis by our team.

Threat Intelligence

Our team harnesses both externally and internally generated intelligence feeds for immediate detection based on known threat activity.

Eyes On Glass Identifying Your Real Risks

Our analyst team is constantly reviewing your data for anomalous behavior and alerting you immediately upon discovery. Alerts generated by our team will provide you with a summary of what's been detected and details around the type of alert.

Indicators Of Execution

Our service utilizes behavioral-based signatures based on profiled malware and threat actor activity that is delivered via your content feeds. Your team is constantly researching emerging threats and developing these signatures to keep up with the dynamic & evolving world of threats.

APPENDIX

Digital Guardian Threat Aware Protection

Next Generation Data Protection

Data protection is at the core of our company mission. Our next generation data protection platform is purpose built to stop data theft. This platform is designed to:

- Discover and protect sensitive data through out the data lifecycle and across the enterprise
- Protect sensitive data on the network at the endpoint, in storage and in the cloud
- Provide automated classification
- Provide integrated advanced protection to protect data from external threats
- Provide flexible deployment options including a managed security service manned by our peerless analyst team with deep, real-world expertise

Management Console

Data Discovery

Data Classification

Advanced Threat Protection

Endpoint Data Loss Prevention

Network Data Loss Prevention

Cloud Data Protection

Free Download

Digital Guardian Platform Technical Overview

Free Download

Digital Guardian Managed Security Program Overview

A Leader In The Gartner Magic Quadrant

- "Digital Guardian is a suitable choice for organizations with strong regulatory compliance concerns, specifically in the healthcare and financial services industries, as well as organizations with intellectual property protection requirements."
- "Digital Guardian is also a strong choice for organizations requiring uniform DLP rules to work equally well across Windows, Mac OS X and Linux operating systems."
- "Clients report faster deployment times and successful projects when utilizing the Digital Guardian product in conjunction with Digital Guardian Managed Services."

Free Download

Gartner 2017 MQ
for Enterprise DLP

2017 Gartner Magic Quadrant For Enterprise Data Loss Prevention

Gartner 2017 Magic Quadrant for Enterprise Data Loss Prevention, 1 February, 2017, Brian Reed and Neil Wynne.

60 MILLION TERABYTES

OF SENSITIVE DATA IS PROTECTED DAILY
BY DIGITAL GUARDIAN AGENTS

OVER
2.5 MILLION
AGENTS DEPLOYED WORLDWIDE

TRUSTED DAILY BY MORE THAN
450
OF THE LARGEST BRANDS IN THE WORLD

ACROSS
54
COUNTRIES

...ONE OF THE LARGEST AND MOST RESPECTED
COMPANIES IN THE WORLD HAS DEPLOYED OVER
300,000 **AGENTS**

INCLUDING...

7 OF THE **TOP 10** PATENT HOLDERS

AND **7** OF THE **TOP 10** AUTO COMPANIES

THE ONLY AGENT-BASED TECHNOLOGY COVERING
250,000 EMPLOYEES
USING A SINGLE MANAGEMENT SERVER

WE ARE THE **DATA PROTECTOR** OF **CHOICE** IN

ENERGY | FINANCIAL SERVICES | GOVERNMENT | TECHNOLOGY | HEALTHCARE & LIFE SCIENCES | MANUFACTURING

BECAUSE WE'RE FOCUSED
ON PROTECTING
ONE THING: DATA

FORTRA™

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

(fta-dg-gd-0523-r1-79d)