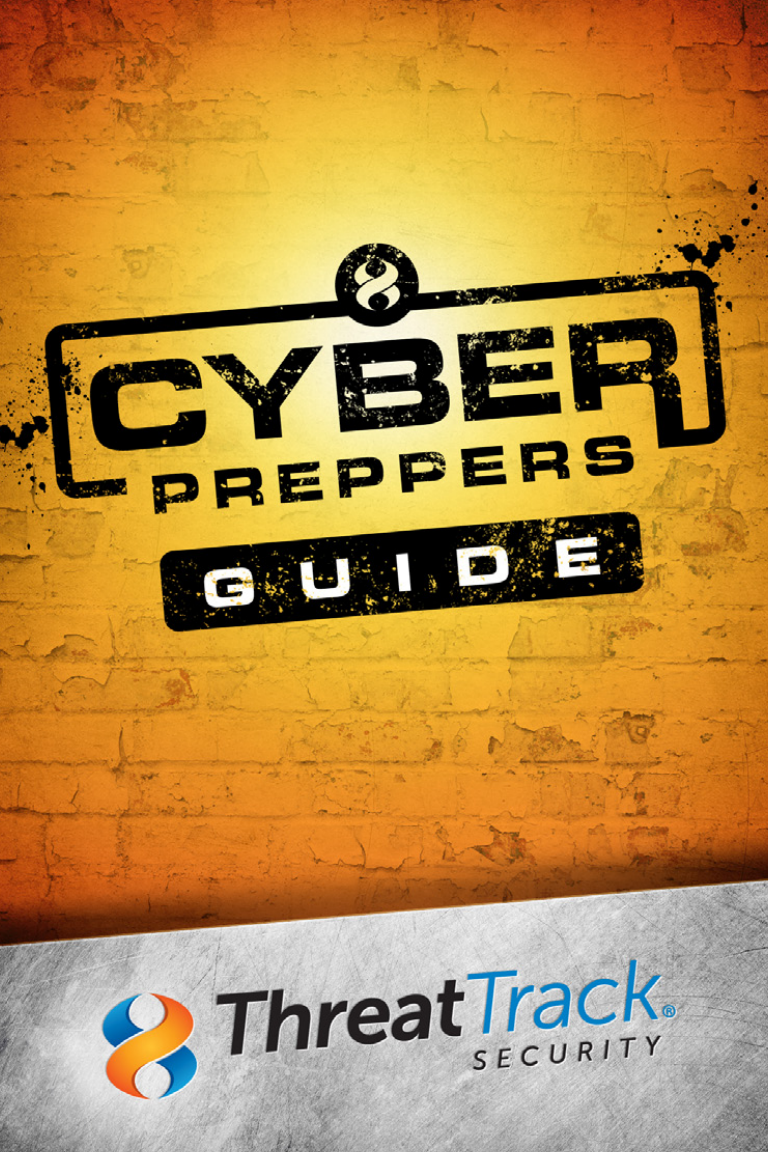
CYBER
PREPPERS
GUIDE
ThreatTrack
SECURITY

WAKE UP!

There is a tectonic shift in cybersecurity underway right now. Sophisticated malware is reshaping the threat landscape, laying waste to yesterday's security best practices and raiding corporate and government networks with impunity.

Become a Cyber Prepper and join ThreatTrack Security in the fight against Advanced Persistent Threats (APTs), targeted attacks and all the other sophisticated malware that easily evades your traditional cyber defenses.

This Cyber Preppers Guide will open your eyes to the new cyber reality and empower you to once again take control of your cybersecurity.

Welcome to the revolution,

The ThreatTrack Security Cyber Preppers

THE CYBER PREPPER RULES

CYBER PREPPER RULE #1
GET YOUR BEARINGS

Does today's **malware** landscape have you worried? If it does, you're not alone. If it doesn't, maybe it should.

200,000+
NEW MALWARE THREATS ARE CREATED EVERY DAY [1]

Top technology and security executives are very concerned about their ability to combat today's malware. Moreover, malware analysts – the professionals with the most experience dealing with these threats – are struggling with the complexity of today's malware and the volume with which it is attacking their organizations.

TOP TECH & SECURITY EXECUTIVES	FRONT-LINE MALWARE ANALYSTS
69% CONCERNED THEY ARE VULNERABLE TO ADVANCED MALWARE THREATS [2]	**67%** CONCERNED ABOUT INCREASING COMPLEXITY OF MALWARE [3]
66% UNSURE IF THEY HAVE BEEN TARGETED BY AN APT [2]	**67%** STRUGGLE WITH VOLUME OF MALWARE THEY FACE [3]
47% DO NOT USE ADVANCED MALWARE ANALYSIS [2]	**35%** LACK ACCESS TO ADVANCED MALWARE ANALYSIS [3]

Priority #1 for any cybersecurity leader is to ensure you're aware of the constantly shifting threat landscape and the implications it holds for your security and your team's ability to meet its objectives.

CYBER PREPPER RULE #2
MIND THE WILD(ER)LIFE

Enterprises face a relentless onslaught of cybercrime and must prepare themselves to combat everything from **cyber-espionage** to **hacktivism** to spear phishing to the millions of variants of viruses, worms, Trojans, bots and malicious email plaguing the Internet right now.

Long gone are the days of malware writers trying to make names for themselves by disrupting operations and just being a nuisance.

75% OF DATA BREACHES ARE FINANCIALLY MOTIVATED [4]

Cybercriminals have gotten organized and much smarter. Cybercrime is a multi-billion dollar economy fueled by sophisticated, disciplined organizations, deploying new weapons and tactics like **Advanced Persistent Threats (APTs)** and **targeted attacks**.

APTs may have risen to prominence in recent years as the security industry's latest boogey man, but targeted attacks are where **threat actors** really demonstrate their expertise to devastating effect.

STATE-SPONSORED CYBER-ESPIONAGE GRABS HEADLINES BUT MAKES UP ONLY 4% OF SECURITY INCIDENTS. THESE THREAT ACTORS ACCOUNT FOR MOST OUTSIDE BREACHES: [5]

32%	14%	12%	10%
HACKERS	COMPETITORS	ORGANIZED CRIME	HACKTIVISTS

Targeted attacks are very precise cyber-attack campaigns aimed at a specific individual's system within an organization. These attacks often use a mix of traditional malware-delivery tactics and **exploits** that only execute on a specific system in order to evade detection and risk alerting the victim. The ultimate objective being to gain control of the system(s) with access to personal data, intellectual property and other valuable information.

CYBER PREPPER RULE #3
IT ONLY TAKES ONE

40% OF DATA BREACHES INVOLVE MALWARE [4]

92% OF DATA BREACHES PERPETRATED BY OUTSIDERS [4]

$3.03 MILLION IS THE AVERAGE COST OF LOST BUSINESS DUE TO A DATA BREACH [6]

The average data breach today compromises **28,765 records**[6]. Trade secrets in industries like high-tech, oil & gas, and manufacturing could be the difference between a sustained competitive advantage or total loss of revenue.

What sensitive data are you responsible for protecting?

Who do you think would be most interested in acquiring it?

When you consider the costs associated with loss of competitiveness, eroded customer trust, government fines and litigation, one breach may be all it takes to put many businesses out of business.

CYBER PREPPER RULE #4
COVER YOUR CLOUD

Your network is changing. The Bring Your Own Device trend is here to stay. We rely more on cloud-based services, online storage and social media, exposing our data to new risks. Yet many still lag in adequately defending all these **attack vectors**. **Only 18%**[5] of enterprises have policies governing cloud computing.

MOST COMMON CAUSES OF BREACHES [7]

30%	28%	27%
SQL INJECTION	TARGETED ATTACKS	ADVANCED MALWARE

To prevent breaches, educate yourself on all the vulnerabilities these new technologies create and how hackers exploit them.

CYBER PREPPER RULE #5
BLAZE YOUR OWN TRAIL

Many organizations look to government and industry compliance standards for guidance.

If you're among the box-checkers only concerned about being "in compliance" in the event of a breach to protect yourself from fines or litigation, then you're just asking for trouble. After all, cybercriminals know this playbook as well as you do, and it was dated the day it was printed.

You need to push beyond the basics of cybersecurity and employ the latest solutions available, including dynamic **malware analysis** and **advanced threat defense** solutions that detect and eliminate APTs and targeted attacks.

ENTERPRISES MAKING ADVANCE THREAT DEFENSE A TOP PRIORITY

CYBERSECURITY INVESTMENT PRIORITIES FOR 2014 INCLUDE: [5]

- THREAT-INTELLIGENCE SUBSCRIPTION SERVICES
- PROTECTION/DETECTION MANAGEMENT SOLUTIONS FOR APTS
- INTRUSION-DETECTION TOOLS
- SECURITY INFORMATION AND EVENT MANAGEMENT TECHNOLOGIES
- SECURITY EVENT CORRELATION TOOLS

Listen to your teams; what solutions are they asking for? Are they just making do with a hodge-podge assembly of disparate open-source tools that malware writers know how to fool? You can do better.

EXPOSE. ANALYZE. ELIMINATE.

ThreatTrack Security delivers the tools and knowledge Cyber Preppers need to defeat advanced malware threats.

THREATSecure™

APT DETECTION AND REMEDIATION

- Automatically detect advanced malware threats that others can't
- Analyze any file type for malicious behavior
- Generate custom remediation signatures for all discovered threats

THREATIQ™

REAL-TIME THREAT INTELLIGENCE

- Access continuous stream of malicious files, URLs and other emerging threats
- Ensure your firewall, IDS/IPS, and other defenses are blocking the latest threats
- Retrieve malware samples for detailed analysis with ThreatAnalyzer

THREATAnalyzer®

ADVANCED MALWARE ANALYSIS

- Identify, profile and stop APTs and targeted attacks
- Analyze files or URLs for malicious behavior
- Know how malware will behave on your network within our customizable environment

VIPRE® BusinessPremium™

ENDPOINT SECURITY

- Antivirus for PCs and Macs
- Low CPU and memory usage
- Integrated patch management
- Mobile Device Management
- Integrated management for Hyper-V environments

WWW.THREATTRACKSECURITY.COM

CYBER PREPPER RULE #6
BLINDERS OFF

Despite your best efforts, you're probably still facing plenty of self-inflicted cyber-wounds.

Don't get too focused on outside threat actors to the point that you don't see and fix the avoidable mistakes your users make, including senior executives.

MALWARE ANALYSTS TELL US THEY HAD TO REMOVE MALWARE FROM SENIOR LEADERSHIP'S PCS OR MOBILE DEVICES FOR THE FOLLOWING REASONS: [3]

- **56%** CLICKED ON A MALICIOUS LINK IN A PHISHING EMAIL
- **47%** ATTACHED AN INFECTED DEVICE TO A PC
- **45%** LET A FAMILY MEMBER USE A COMPANY COMPUTER
- **40%** VISITED AN INFECTED PORNOGRAPHIC WEBSITE
- **33%** INSTALLED A MALICIOUS APP

CYBER PREPPER RULE #7
BE SELF-RELIANT

"WHILE INFORMATION SECURITY RISKS HAVE EVOLVED AND INTENSIFIED, SECURITY STRATEGIES – HISTORICALLY COMPLIANCE-BASED ... HAVE NOT KEPT PACE." [5]

Don't wait for others to tell you what to do. While politicians debate cybersecurity policy and grandstand over headline-grabbing breaches, your risk and exposure only grows.

You need to take the initiative, but that doesn't mean you go it alone. **Nearly 30%**[5] of enterprise cybersecurity professionals do not collaborate with others to improve security.

The more cybersecurity professionals collaborate and share information, the stronger our collective defenses will become.

CYBER PREPPER RULE #8
CHANCE IS NOT STRATEGY

If you don't have the right tools in place, your chances of proactively discovering or preventing a breach plummet.

Only **10%** of data breaches are discovered by accident. Most are discovered through the use of forensic investigative tools like a malware analysis sandbox, **28%**; DLP solution, **19%**; or through law enforcement notification after the fact, **15%**.[7]

66% OF DATA BREACHES TAKE MONTHS TO BE DISCOVERED.[4]

Put the right tools in place and ensure your cyber defense and breach-detection capabilities are a sure thing.

But don't lose sight of the fact that a strong strategy also involves the right mix of tools and people. An effective cyber defense also needs a strong leader. If you're organization is among the **35%**[5] of enterprises without a **Chief Information Security Officer (CISO)**, that should be your #1 priority.

#2 on your list should be establishing an **Incident Response Team (IRT)** and staffing it with experienced cybersecurity professionals. **42%**[2] of senior executives say their organization does not have an IRT to respond to cyber-attacks.

Next, conduct that thorough risk assessment of your organization. The best tools and people are useless if you don't know what you're defending.

Finally, put it all on paper and develop your formal cybersecurity and incident response strategy.

CYBER PREPPER RULE #9
LEARN TO FORAGE

GOOD NEWS. INFORMATION SECURITY BUDGETS ARE ON THE RISE, BY AS MUCH AS 51%.[5]

BAD NEWS. INFORMATION SECURITY REMAINS AT LESS THAN 4%[5] **OF OVERALL IT SPENDING.**

As a cybersecurity leader in your organization, you need to make the case for necessary investment to protect your operation in an increasingly dangerous online world.

Now is the time to act. Senior leadership – from the CEO and CFO to the Board of Directors – have never been more aware of cybersecurity than they are right now.

You know there's money in that hefty IT budget. Get creative and ensure that cybersecurity gets its share as well.

CYBER PREPPER RULE #10
START A NERD GANG

The only way you're going to outsmart and outmuscle today's cyber-thugs is with your own gang of cyber-toughs.

This means recruiting new expertise to the team, but cybersecurity is an in-demand skill right now, and there is a definite shortage out there. You may have luck finding members of your IT team you can train up and build your gang from within, and take advantage of new synergies and silo-breaking you can accomplish between the offices of the CISO and CIO.

With the right gang, nobody will mess with you.

GLOSSARY

Advanced Persistent Threats (APTs) – Sophisticated cyber-attacks that compromise systems and networks for malicious purposes; primarily characterized by their ability to operate and avoid detection for an extended period of time.

Advanced threat defense – Emerging cybersecurity solutions that can detect and eliminate APTs and other forms of sophisticated malware.

Attack vector – The channel or path through which a hacker or cybercriminal compromises a network to deliver malware.

Chief Information Security Officer (CISO) – A senior executive designated responsible for an organization's information security and cybersecurity strategy.

Cyber-espionage – The stealing of personal, proprietary or classified information via cyber-attack methods such as APTs or other malware; typically associated with spying among nation states or by foreign competitors.

Exploits – Often referred to as Zero-day threats, take advantage of vulnerabilities in the software code of popular applications like Adobe Reader, Java and more to propagate malware.

Hacktivism – Politically motived cyber-attacks generally launched to disrupt operations and to gain notoriety.

Incident Response Team (IRT) – Specially trained personnel within an enterprise or government agency charged with responding to and defending organizations from cyber-attacks.

Malware – Encompassing viruses, Trojans, bot nets, worms, rootkits, keyloggers, adware, ransomware and more, this malicious software code infects networks and disrupts operations typically for financial gain.

Malware Analysis – A subset of cybersecurity solutions such as a sandbox that enables users to analyze the behavior of malware, reporting on systems changes made, network traffic generated and more; customized malware analysis environments are the most effective countermeasure to targeted attacks; can be deployed for forensics purposes in post-breach analysis.

Targeted attacks – Complex, multi-stage cyber-attacks that target specific users or system configuration in an organization for the purpose of compromising system(s) with access to sensitive information.

Threat actor(s) – The person, people or entities perpetrating cyber-attacks, such as hackers, members of cybercrime groups or individuals within state-sponsored organizations.

REFERENCES

1 ThreatTrack Security Labs

2 ThreatTrack Security; *Enterprise Executives Lack Confidence About Cybersecurity, 2013*

3 ThreatTrack Security; *Malware Analysts Have the Tools They Need, But Challenges Remain, 2013*

4 Verizon; *2013 Data Breach Investigations Report*

5 PwC; *Global State of Information Security Survey 2014*

6 Ponemon Institute; *2013 Cost of Data Breach Study: Global Analysis*

7 Ponemon Institute; *The Post Breach Boom, 2013*

ABOUT THREATTRACK SECURITY

ThreatTrack Security specializes in helping organizations identify and stop Advanced Persistent Threats (APTs), targeted attacks and other sophisticated malware that are designed to evade the traditional cyber defenses deployed by enterprises and government agencies around the world. The company develops advanced cybersecurity solutions that expose, analyze and eliminate the latest malicious threats, including its ThreatSecure advanced threat detection and remediation solution, ThreatAnalyzer malware behavioral analysis sandbox, ThreatIQ real-time threat intelligence service, and VIPRE business antivirus endpoint protection.

Learn more at www.ThreatTrackSecurity.com

33 North Garden Avenue, Suite 1200
Clearwater, FL 33755

www.ThreatTrackSecurity.com