FireEye™

White Paper

Thinking Locally, Targeted Globally

New Security Challenges for State and Local Governments

Contents

Introduction

In the new era of cyber warfare, states, cities, and towns are directly in the crosshairs.

Never before have state and local governments been expected to do so much with so little. Even as budgets remain tight in a post-recession environment, tech-savvy citizens demand higher levels of service. The want to pay taxes by credit card, renew their driver's license online, and check traffic from their smartphone.

These responsibilities make cyber security critical for state agencies, municipalities, and public utilities. Governments possess residents' most sensitive information—including inviolable personal data such as Social Security numbers and birth certificates.

"Personal data tends to be undervalued," said Clifford Clarke, CIO of the Public Technology Institute (PTI), in a recent interview with public policy magazine Governing the States and Localities. "Some municipalities don't think they have anything to protect."[1]

Equally imperative for state and local governments is safeguarding critical infrastructure. Dams, freeway systems, power and water plants, airports, and emergency communication, are among the vital assets that fall under state or local purview.

These critical systems and the highly sensitive data they contain are enticing targets for cybercriminals and foreign governments. State and local governments face a growing torrent of attacks that are growing increasingly sophisticated, stealthy, and dangerous. According to Gen. Keith B. Alexander, who heads the National Security Agency and the U.S. Cyber Command, the number of cyber attacks on U.S. infrastructure jumped 17-fold between 2009 and 2011.[2]

U.S. officials, including President Barak Obama, have grown increasingly alarmed by the threat of attacks against state and municipal governments. In an editorial urging congress to pass the Cybersecurity Act of 2012, a law designed to strengthen cyber defense, Obama warned that "computer systems in critical sectors of our economy are being increasingly targeted."

"The lack of clean water or functioning hospitals could spark a public health emergency," he wrote. "And as we've seen in past blackouts, the loss of electricity can bring businesses, cities, and entire regions to a standstill."[3]

In 2012, U.S. Defense Secretary Leon Panetta warned of a looming "cyber Pearl Harbor" surprise attack against utilities or transportation systems. He cited online breaches that have already occurred of control systems for chemical, water, and electrical plants, as well as public transportation control software.[4]

National Intelligence James Clapper echoed those sentiments in March 2013 testimony to the U.S. Senate Select Committee on Intelligence. "In some case, the world is applying digital technologies faster than our ability to understand the security implications and mitigate potential risks," he said.[5]

[1] Tod Newcombe (Governing the States and Localities). "Cybercrime Hits Small Towns." December 2011.

[2] David E. Sanger and Eric Schmitt (The New York Times). "Rise Is Seen in Cyberattacks Targeting U.S. Infrastructure." July 2012.

[3] Barak Obama (The Wall Street Journal). "Taking the Cyberattack Threat Seriously." July 2012.

[4] Chris Carroll (Stars and Stripes). "US can trace cyberattacks, mount pre-emptive strikes, Panetta says." October 2012.

[5] Mark Mazzetti and David E. Sanger (New York Times). "Security Leader Says U.S. Would Retaliate Against Cyberattacks." March 2013.

And former U.S. Department of Homeland Security Secretary Janet Napolitano, in her farewell address, warned of "a major cyber event that will have a serious effect on our lives, our economy, and the everyday functioning of our society."[6]

In the first half of 2013, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) responded to more than 200 incidents across critical infrastructure sectors—more than twice the volume of attacks in all of 2012—with half of those targeting electrical utilities.[7]

State computers in Utah alone are attacked as much as 20 million times a day by cybercriminals using automated systems, said Mark VanOrden, the state's chief information officer and executive director of the Utah Department of Technology Services. The figure (which likely includes reconnaissance by attackers) is up from about a million attacks per day in 2011.[8]

In May 2013, the U.S. Department of Homeland Security warned local governments that they were among the hundreds of high-profile targets identified by a group of Middle East- and North Africa-based criminal hackers known as "OpUSA."[9]

At the same time, many state and local agencies are not ready for the inevitable assault. In a recent survey, 44 percent of federal, state, and local government IT workers said their infrastructure was not prepared for cyber attacks.[10]

This paper outlines the inexorable upsurge in cyber attacks, why traditional defenses have not kept pace with advanced attackers, and how state and local governments can better defend their data and critical infrastructure.

[6] U.S. Department of Homeland Security. "Remarks by Secretary of Homeland Security Janet Napolitano at the National Press Club." August 2013.

[7] ICS-CERT Monitor. "Brute Force Attacks on Internet-Facing Control Systems." June 2013.

[8] Shara Park (KSL TV). "State faces millions of cyber attacks per day, department head says." July 2013.

[9] U.S. Department of Homeland Security. "OpUSA: Criminal Hackers Planning Cyber Attacks Against US Websites." May 2013.

[10] Consero Group. "2013 Government IT Data Survey." April 2013.

Advanced Persistent Threats: The New Normal

Today's cyber attacks have changed radically from just a few years ago. Broad, scattershot attacks designed for mischief have been replaced with attacks that are advanced, targeted, stealthy, and persistent. The new generation of attacks, sometimes known as advanced persistent threats (APTs), are focused on acquiring something valuable—sensitive personal information, intellectual property, authentication credentials, insider information, and the like. Many advanced attacks cut across multiple threat vectors—Web, email, file shares, and mobile devices—and unfold in multiple stages, with calculated steps to get in, signal back out of the compromised network, and get valuables out.

These attacks are well funded and organized. And they easily bypass traditional defenses such as traditional and next-generation firewalls (NGFW), intrusion prevention systems (IPS), anti-virus (AV), and gateways. These defenses, built for a previous generation of attacks, rely heavily on malware signatures and known patterns of behavior. That approach leaves these defenses vulnerable to fast-moving, ever-evolving threats that exploit previously unknown, zero-day vulnerabilities.

APT attacks on state and local governments have become all too frequent in recent months. A data breach of a state's department of revenue system last year cost the state more than $20 million, including the costs of remediation and preventative measures.[11]

And in December 2012, a well-known hacking group in China infiltrated a decoy water-control system created by cybersecurity researchers. Between March and June of 2013, 12 honeypots deployed across eight different countries attracted 74 intentional attacks. Of these attacks, 10 were sophisticated enough to wrest complete control of the dummy control system.[12]

In a recent case-study interview, the chief information security officer of a major U.S. city said he sees a clear increase in attempts by other nation-states to disrupt critical U.S. infrastructure. His city is responsible for major dams, regional utilities, emergency services, and a multi-agency communications system.

"If it's organized crime trying to steal someone's bank password, that's bad enough," the CISO said. "But if you knock down a 911 center, people are going to die."[13]

And even non-catastrophic breaches can be costly. According to the Ponemon Institute,[14] the average U.S. breach cost targeted organizations $5.4 million, or $188 per breached record.

[11] Tim Smith (The Greenville News). "DOR seeks $20 million loan to cover data breach expenses." December 2012.

[12] Kyle Wilhoit. "The SCADA That Didn't Cry Wolf." July 2013.

[13] Interview from FireEye customer case-study interview.

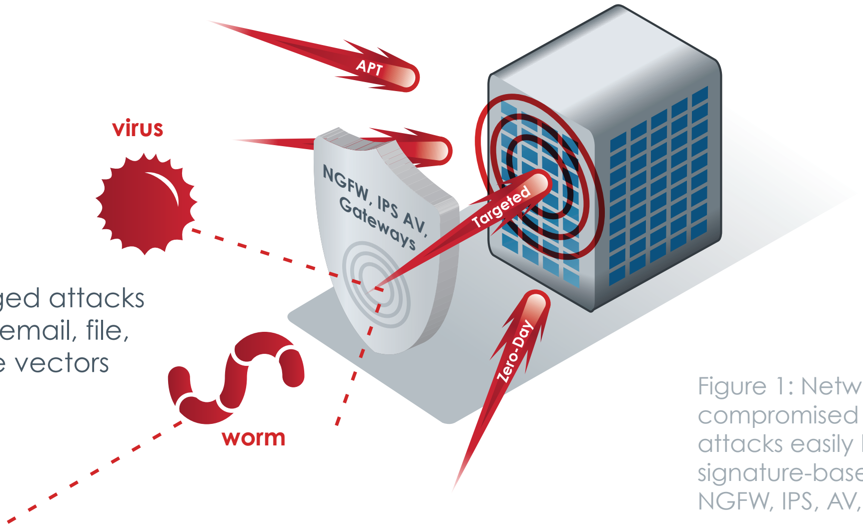
[14] Ponemon Institute. "2013 Cost of Data Breach Study: Global Analysis." May 2013.

Why Traditional Tools Fail To Detect Advanced Attacks

Why are so many compromises occurring? In large part, because the defenses that many state and local governments have in place today are ill equipped to combat today's advanced attacks. While firewalls, NGFW, IPS, AV, and gateways remain important security defenses, they continue to be proven ineffective at stopping today's attacks.

Signatures and blacklists are ineffective

These technologies rely on approaches such as URL blacklists and signatures. By definition, these approaches cannot stop dynamic attacks that exploit zero-day vulnerabilities. If an IPS or AV solution does not match the signature of a new exploit, it cannot stop it. When highly dynamic malicious URLs are employed, URL blacklists do not cut it. Traditional defenses stop known attacks. But they are rendered defenseless against "unknown" advanced targeted attacks.



Multi-pronged attacks from Web, email, file, and mobile vectors

Figure 1: Networks are being compromised as advanced attacks easily bypass traditional signature-based defenses like NGFW, IPS, AV, and gateways.

Sandboxes: a new tack with the same old flaws

Sandboxes, often touted as an alternative to traditional defenses, suffer many of the same shortcomings. Rather than adopting a truly fresh approach, most vendors merely graft a sandbox onto their legacy strategies, which routinely fail to catch advanced attacks.

Many sandboxes are rooted in widely available hypervisors that malware can easily detect and evade. And most sandboxes rely on file-based analysis—an approach that can miss the exploit phase of an attack and the multiple threat vectors used in today's sophisticated attacks.

The Multi-Vector, Multi-Stage Nature of Today's Attacks

Advanced attacks often comprise of a number of distinct, yet coordinated stages, and often use multiple attack vectors. They can be delivered through websites, email, files shares, and mobile devices, they can be blended (for example, email-based attacks that contain malicious URLs), and they can exploit application and OS vulnerabilities.

The following list describes the different stages that typically comprise these coordinated attacks:

- **System exploitation.** Leveraging zero-day exploits or targeted spear-phishing tactics, or sometimes both, advanced attacks can effectively compromise specific systems—the critical first step of the campaign.
- **Malware download.** Once a system has been exploited, the attacker downloads a malicious executable, such as a key logger, Trojan backdoor, password cracker, or file grabber. Just one initial exploit can translate into dozens of infections on the same system.
- **Control established.** Once the malware installs, the attacker has cracked the first step to establishing a control point from within your defenses. Once in place, the malware calls out to criminal servers for further instructions. Malware can also replicate and disguise itself to avoid detection during scans. Some malware turns off AV scanners, reinstall any missing malware components after a cleaning, or lie dormant for days or weeks. By using callbacks from within the trusted network, malware communications are allowed through the firewall and various network layers. At this point, the criminal has established long-term control over systems.
- **Data exfiltration.** Next, data acquired from infected servers is staged for exfiltration. Data can be exfiltrated over commonly allowed protocols, such as FTP or HTTP. During this process, the criminal may encrypt communication to disguise the assets being transmitted. Or the criminal may send data to another compromised machine outside the targeted organization, for example at a hosting provider, to further disguise their identities and whereabouts.
- **Lateral movement.** During this phase, the criminal works to move beyond the system initially exploited, and begins to move laterally within the target organization. The attacker accesses additional systems and gains elevated permissions to important user, service, and administrative accounts. To do so, they may leverage automated, self-replicating malware to infect multiple network assets.

Combatting Advanced Attacks

To address these attacks and protect critical infrastructure and data, state and local governments must be able to:

- Detect and stop advanced attacks that exploit zero-day vulnerabilities—when they first appear on the network.
- Expose the entire cyber attack life cycle by correlating intelligence across various threat vectors and stages.
- Produce complete cyber forensic details of attacks that exploit Web, email, file, mobile, or hybrid attack vectors.

Why State and Local Governments Are Choosing FireEye

Clearly, state and local governments need a next-generation threat prevention platform, one that identifies and blocks the new breed of cyber attacks. That is why many of the top agencies are turning to FireEye. With the FireEye Threat Prevention Platform, state and local governments get the multi-faceted, coordinated defense capabilities they need to guard against sophisticated attacks including zero-day and APT attacks. The following sections detail how FireEye delivers effective protection.

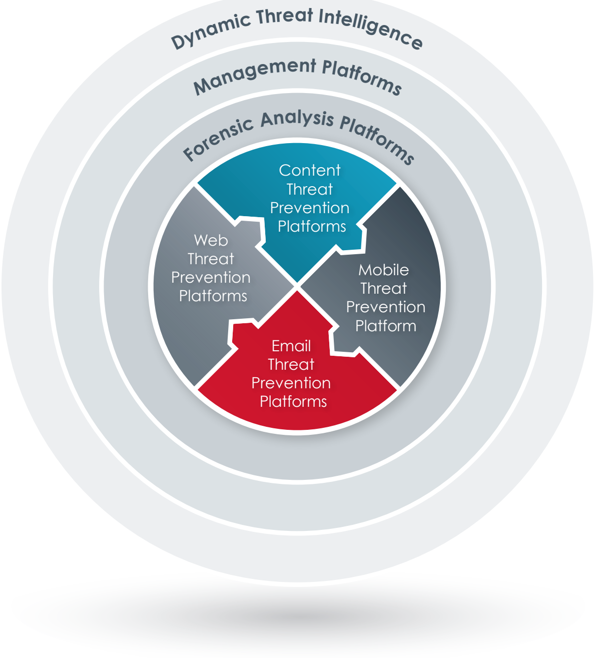

Dynamic Threat Intelligence
Management Platforms
Forensic Analysis Platforms
Content Threat Prevention Platforms
Web Threat Prevention Platforms
Mobile Threat Prevention Platform
Email Threat Prevention Platforms

Figure 2: Complete protection against advanced targeted attacks for Web, email, files, and mobile.

Gain A Cohesive, Correlated View of All Major Threat Vectors—Web, Email, File Shares, and Mobile

With the FireEye platform, organizations get a real-time correlated view of all the potential threat vectors that cybercriminals use, including:

- **Web.** Browser-based threats and malicious communications can take many forms and move across a range of protocols, including FTP, HTTP, and IRC. The FireEye NX series tracks sites and communications in real time, across these different protocols to thwart advanced attacks.
- **Email.** Spear-phishing emails represent one of the most common approaches for launching an advanced attack on state and local governments. The FireEye EX series can guard against these types of threats, providing real-time analysis of URLs in emails, email attachments, and Web objects to determine whether they are malicious.
- **File Shares.** Even if Web and email channels are secured, malicious files can still make it into a corporate network in any number of ways—through a USB drive, a mobile device, download from a cloud service, and many more. These malicious files can be purposely or inadvertently saved to any number of locations throughout an organization, and even lie dormant for a certain period before they exhibit their malicious behavior. The FireEye FX series detects and eliminates malware resident on file shares.
- **Mobile.** Malware targeting mobile devices jumped 614 percent between March 2012 and March 2013, and more than 500 third-party app stores contain malicious apps, according to Juniper Networks.[15] Security researchers found more than 51,000 new mobile malware threats in the first half of 2013 infecting about 21 million devices.[16] Mobile malware can do everything from exfiltrate sensitive data[17] to secretly record video and audio.[18] FireEye Mobile Threat Prevention identifies apps with malicious or unwanted behavior.

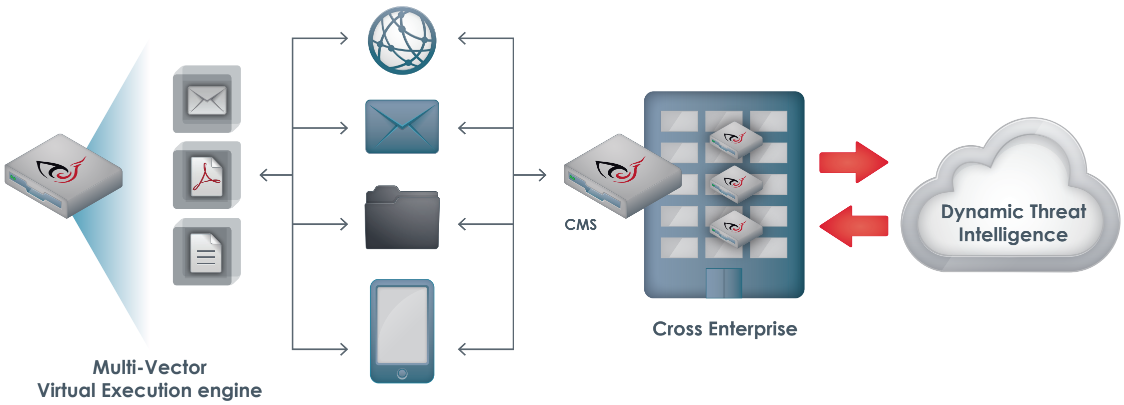


Figure 3: FireEye advanced threat protection architecture

[15] Juniper Networks. "Third Annual Mobile Threats Report." June 2013.

[16] NQ Mobile. "2013 Mid-Year Mobile Security Report." July 2013.

[17] Yacin Nadji, et al. "Automated Remote Repair for Mobile Malware." December 2011.

[18] Josh Halliday. "App for Google Android smartphones secretly records calls." August 2011.

Most important, the FireEye CM series correlates all of the threat intelligence generated from the FireEye platforms. For example, to guard against sophisticated spear-phishing attacks, security teams need capabilities for discovering a Web-based attack in real time, tracing the initial email that spawned the attack, and then doing the analysis required to determine if others within the organization have been targeted. By providing this kind of correlation, the FireEye CM platform can deliver timely, actionable information about current threats and how to stop them. Further, the FireEye CM platform inspects across many protocols and throughout the stack, including the network layer, operating systems, applications, browsers, and plug-ins such as Flash. This capability enables state and local governments to effectively defend their networks.

Leverage Signature-Less, Real-Time Security That Thwarts Zero-Day Attacks

The FireEye platform provides dynamic, real-time analysis of network traffic and processes, rather than just comparing bits of code to signatures. This signature-less analysis is critical to detecting and stopping polymorphic malware on the Web as well as malware hosted on dynamic, fast-changing domains.

If suspicious code is detected, the FireEye platform executes it in a purpose-built, instrumented environment. Malware activities are monitored at every layer in the technology stack, from active memory to browser plug-ins. With this full-spectrum testing, the FireEye platform can irrefutably determine the intention and activities of the attacker, zeroing in on real threats and minimize false positives and false negatives.

Guard Against Malicious Code Installs and Block Callbacks

To combat advanced attacks effectively, systems must identify whether malware binaries, executable files, and callback communications are malicious. This requires monitoring outbound host communications over multiple protocols in real time. Organizations must analyze not just the destination IP or domain name, but also the unique characteristics of the communication protocols employed.

The FireEye platform addresses these key requirements. Once malicious code is flagged, the FireEye platform blocks its communication ports, IP addresses, and protocols to halt any dangerous transmissions. When the binary of zero-day malware has been captured, the FireEye platform gathers and disseminates the threat intelligence organizations need to block subsequent attacks that use the same binary file.

Harness Timely, Actionable Threat Intelligence and Malware Forensics

Once malicious code has been analyzed in detail, the FireEye CM platform helps ensure that the information gathered is fully leveraged. With the FireEye CM platform, organizations can leverage this information for a number of purposes:

- Security analysts can use the fingerprint of the malicious code to identify and remediate compromised systems and prevent the infection from spreading.
- Forensics researchers can individually run files through automated off-line tests to confirm and dissect malicious code.
- Malware analysis can be shared with other FireEye and partner products within your organization using the FireEye Dynamic Threat Intelligence™ (DTI) Enterprise. DTI Enterprise empowers a unified, coordinated defense across various threat vectors.
- Additionally, the FireEye DTI cloud network provides real-time global exchange of threat intelligence. The DTI cloud shares information on new threats from participating nodes around the globe.

Conclusion

Today's advanced attacks represent an immediate and dire threat to state and local governments. Unless additional safeguards that effectively thwart these sophisticated attacks are deployed, agencies increasingly run the risk of devastating breaches that compromise confidential or classified info or critical infrastructure. By providing real-time, coordinated security capabilities that thwart today's advanced attacks, the FireEye platform enables state and local governments to safeguard their critical and sensitive assets.

To learn more about how FireEye can help your agency detect and block advanced threats visit: www.fireeye.com

About FireEye, Inc.

FireEye has invented a purpose-built, virtual machine-based security platform that provides real-time threat protection to enterprises and governments worldwide against the next generation of cyber attacks. These highly sophisticated cyber attacks easily circumvent traditional signature-based defenses, such as next-generation firewalls, IPS, anti-virus, and gateways. The FireEye Threat Prevention Platform provides real-time, dynamic threat protection without the use of signatures to protect an organization across the primary threat vectors, including Web, email, and files and across the different stages of an attack life cycle. The core of the FireEye platform is a virtual execution engine, complemented by dynamic threat intelligence, to identify and block cyber attacks in real time. FireEye has over 1,100 customers across more than 40 countries, including over 100 of the Fortune 500.