COMMUNITY PROTECTION

SECURITY IN NUMBERS

WHITE PAPER

FireEye

WHEN IT COMES TO CYBER SECURITY, GOING IT ALONE IS A DAUNTING TASK. AN ISOLATED ORGANIZATION HAS LIMITED KNOWLEDGE, VISIBILITY AND RESPONSES.

AN ACTIVE SECURITY COMMUNITY USES THE EFFORTS OF EVERY MEMBER TO BOLSTER OVERALL CYBER SECURITY INTELLIGENCE.

Neighborhood watch groups are designed to prevent crimes by creating a community of involved citizens that work with local law enforcement to report and investigate suspicious activity. Every day, homeowners and renters monitor activity, report crime and help to make their neighborhoods safer.

These neighborhood groups tap into the knowledge and resources of law enforcement that routinely track criminals, review crime reports and identify patterns of activity. The result? Individual homes are made more secure because the entire community of citizens, law enforcement and private security organizations work together toward the common goal of eliminating crime.

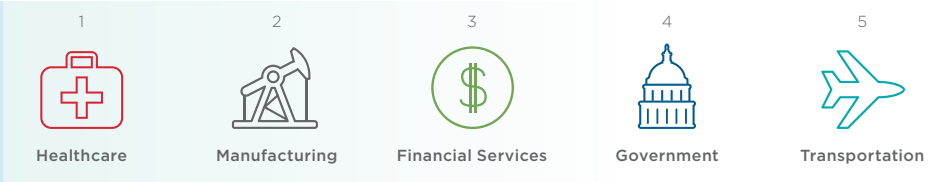
The concept of community also applies to strengthening cyber security. Organizations benefit by becoming a part of a community that faces similar types of security challenges and risks. In the same way that a neighborhood watch is supported by law enforcement agencies, a community is dramatically and consistently effective if it is facilitated and supported by a partner with access to broad and deep threat intelligence and expertise around the world. Working together, the community provides early and extended visibility into threats through knowledge based on extensive experience, current insight and a robust technology foundation. And this actionable visibility can enable the community to quickly analyze incidents, identify attack patterns and incorporate threat intelligence into future protective services and solutions.

COMMUNITIES UNDER ATTACK

History has shown that cyber attacks come in clusters or waves and target specific communities based on industry, location or political association.

For example, healthcare was the industry most targeted by cyber attacks in 2015. Healthcare organizations occupied three of the top seven spots for largest breaches in the same year.[2] Previously, financial services were in the cyber crime spotlight and retailers faced a string of high-profile breaches.

FIGURE 1: THE 5 MOST CYBER-ATTACKED INDUSTRIES IN 2015



Many public and private sector organizations face geopolitical issues, which also shape the cyber threat landscape. During the recent U.S. election cycle, the Washington, D.C., area was home to several geopolitical targets as Russian hackers reportedly attacked Washington think tanks and the Democratic National Committee's computer network.[3]

MUST-HAVE CRITERIA FOR BUILDING COMMUNITY PROTECTION

A community designed and developed to fight cyber crime that enhances the security of every member is hard to find. It's not as simple as joining an industry association. You need a community network committed to gathering and sharing intelligence, enhanced with personnel and infrastructure that actively tracks

You need a community network committed to gathering and sharing intelligence.

adversaries and monitors victims on the front lines. Individual members can attempt to do this alone, but few have the security and intelligence expertise, and most lack the comprehensive visibility of an entire community. Organizations engaged with the community must therefore collect, analyze and then quickly codify the intelligence for use in active security solutions. And ideally, a robust community should be large enough and have the supporting infrastructure to provide visibility across the entire attack lifecycle and deliver protection superior to what any one organization can achieve on its own.

1 Steve Morgan, "Top 5 Industries At Risk Of Cyber-Attacks," *Forbes*, May 13, 2016.
2 Rudy Takala, "Russian hackers reportedly target Washington think tanks," *Washington Examiner*, August 29, 2016.
3 Spencer Ackerman and Sam Thielman, "US officially accuses Russia of hacking DNC and interfering with election," *The Guardian*, October 8, 2016.

An active, robust community

When it comes to cyber security, going it alone is a daunting task. An isolated organization has limited visibility into the threats that it faces, let alone the techniques necessary to defend against them. In an active security community, the efforts of every member can be used to help monitor, analyze, facilitate and extend every other member's cyber security intelligence. The critical data that each member collects as it identifies threats, responds to incidents and analyzes breaches can be redistributed to the rest of the community. If an organization is able to identify and build context for a threat, this knowledge can also be codified and disseminated to the community in real time. A security community can share advance information on attack origin or target, deliver automated proactive protection and provide guidance on the latest methodologies, tools and trends so members can stay ahead of attackers.

Every member benefits from the larger knowledge base of major breaches, attackers, techniques, patterns and the increased visibility contributed by its membership.

The strength of a community grows along with the number, value and resources of individual members. Robust communities have footprints large enough to expand each member's visibility and context. They have more organizations that protect sensitive assets, possess sophisticated security programs to detect and create artifacts, and are tested by frequent and targeted attacks. Even the smallest of organizations can see and benefit from the experience of members in different industries and geographic regions. Every member benefits from the larger knowledge base of major breaches, attackers, techniques, patterns, and the increased visibility contributed by its membership.

An accomplished, trusted security partner

Identifying, organizing and sustaining community protection is a full-time endeavor. Just as law enforcement agencies provide their authority, support and dedicated investigative expertise to their citizenry, organizations need a security partner with proven credentials to help establish, maintain and enhance community protection.

Partners should have the ability to gather and process real-time threat intelligence from individual members to benefit the entire community. The best-equipped partners extend the insights of a community with broad and deep threat intelligence that they have independently gathered, analyzed and produced. These insights will often require extended visibility into attackers, infrastructure and tools to store and analyze collected data, and experts who have the know-how to track and analyze attacker activity to produce immediately actionable insights.

FIREEYE PROVIDES COMPLETE COMMUNITY PROTECTION

FireEye technology, intelligence and expertise are designed to develop and sustain robust communities with a large, active network of analysts dedicated to fighting cyber attacks. No other security company offers your organization a similar breadth or depth of community protection.

Always-on, dynamic network

FireEye has over 160 intelligence analysts around the world who are deeply embedded where attackers plan, design and execute their attacks from Eastern Europe and the Middle East to the Far East. The company also has over 1,000 experts – malware analysts, geopolitical experts and linguists – who understand the context behind the threats and then analyze and correlate observed activity within a highly flexible and scalable threat analysis and machine-learning infrastructure. FireEye insights are derived from more than 10 years of experience responding to the world's most consequential breaches and the Multi-Vector Virtual Execution (MVX)-driven technology that identifies never-before-seen attacks. They allow FireEye to understand how attackers infiltrate an organization, what they do after they breach organizational defenses and how existing security controls might fail.

These expert findings are codified into hourly technology updates and provide the FireEye community with real-time visibility into known and unknown threats. FireEye maps and continues to track nearly 600 million interconnections between threats, as well as the identities, tactics, techniques and procedures of the actors and sponsors behind them. This analysis has enabled FireEye to track over 16,000 threat actors, including more than 30 nation-state sponsored groups, ranging from APT1 to the attackers behind the major breaches found in headlines today. FireEye dossiers help community members to include the threats from these actors in their risk assessment and influence the design and operation of their security programs. This knowledge is also used to build industry-leading products and services that are effective against these threats.

Broad, high-impact footprint

FireEye underpins a security ecosystem that includes 65% of the Fortune 500 and more than 825 of the Global 2000. Its customers represent most of the top ten companies in industries such as retail, healthcare, high-tech, telecommunications, energy and insurance. FireEye analysts and geopolitical experts speak 29 different languages and understand the customs and cultures of multiple countries. The company gathers and uses global intelligence on adversaries, spends nearly 200,000 hours helping breach victims and has more than 5,000 customer deployments of its technology and services. All of these intelligence sources help FireEye to better analyze, respond to and reduce cyber threats. FireEye codifies its understanding of attackers into real-time protection against new attack techniques. The company also give its customers the contextual intelligence they need to know what threats to expect and how to respond to them. With its reach and depth, it can take a threat discovered in one part of its ecosystem and drive protection to all other customers within minutes.

FireEye Customers: % of Top Ten by Industries

80%
CPG/Retail

60%
Defense/Aerospace/Airlines

70%
Energy

80%
Healthcare

80%
High Tech

70%
Insurance

60%
Media/Entertainment/Hospitality

80%
Telecommunications

70%
Utilities: Gas and Electric

70%
Petroleum Refining

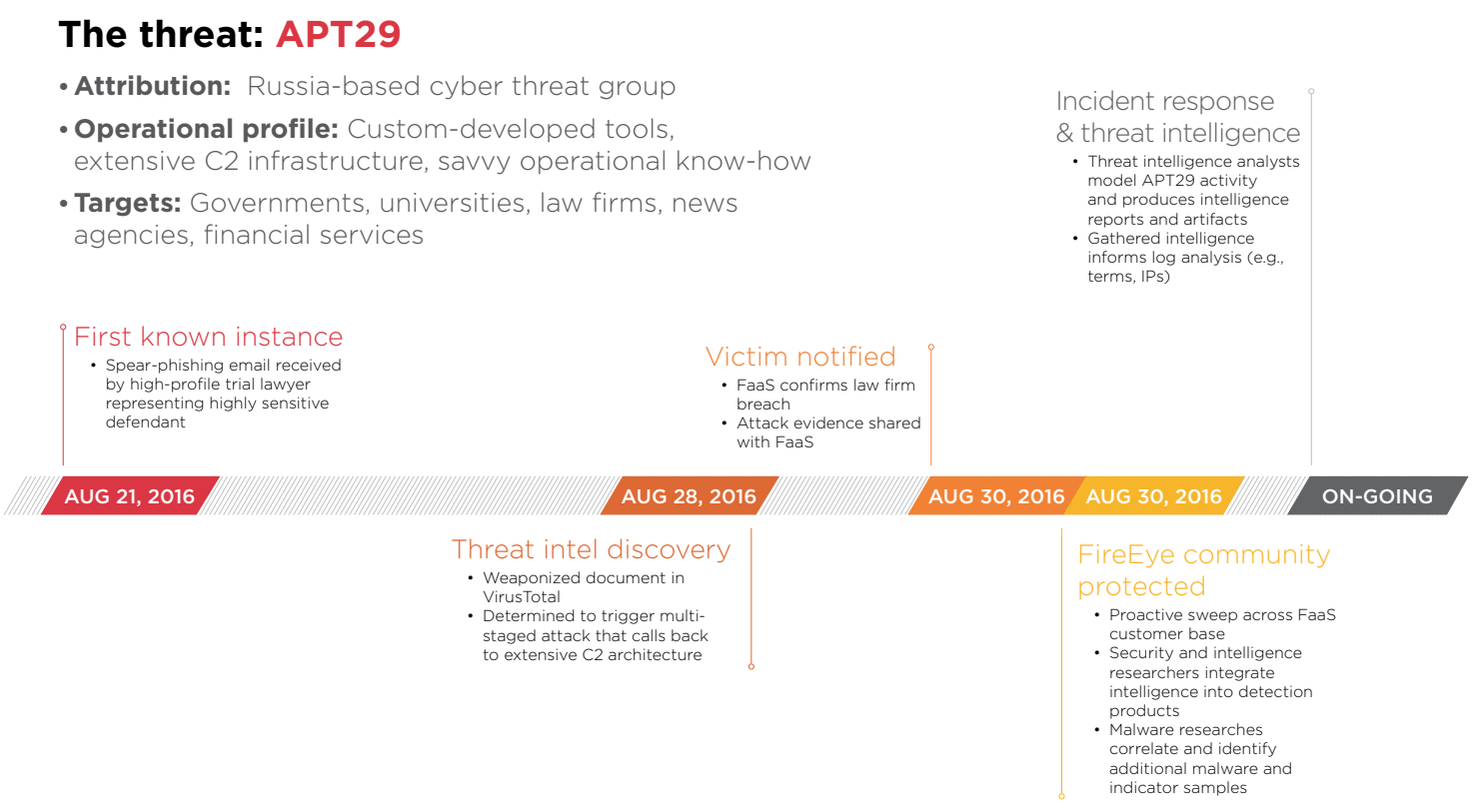
APT29 CASE STUDY: FIREEYE COMMUNITY PROTECTION IN ACTION

In 2015, a law firm with high-profile customers involved in sensitive cases was targeted by a spear-phishing email. Because the targeted company was a customer of FireEye as a Service, FireEye could collect artifacts and evidence including the original spear-phishing email. FireEye analyzed and correlated the evidence to APT29, a Russian-based cyber threat group it had been tracking. APT29 was discovered to have sophisticated custom-developed tools, an extensive command and control infrastructure and savvy operational know-how. FireEye correlated the observed activity to an extensive dossier on APT29 to identify their probable next steps. FireEye then notified the victim and helped them focus their response.

At the same time, FireEye expanded protection against APT29 across its entire customer base. Security and intelligence researchers quickly integrated the new knowledge into deployed FireEye detection products. Combining years of intelligence about this particular threat actor with characteristics specific to this attack, FireEye identified a subset of industries that were at particular risk. FireEye as a Service customers within these industries were placed under heightened attention, received proactive sweeps for threat activity within their environment, and were given threat briefings through their Engagement Managers.

The end result was that more FireEye customers – the community – were protected faster to more quickly recognize indicators and the full scope of any future attacks.

FIGURE 2: THE FIREEYE COMMUNITY PROTECTS MEMBERS WITHIN DAYS AGAINST APT29



PUTTING COMMUNITY PROTECTION TO WORK

An active neighborhood watch group can make your home a safer place. Similarly, your organization can recognize the advantages of belonging to a robust, active community committed to fighting cyber crime. As a trusted security partner, FireEye is uniquely positioned to deliver community protection to you as a member of its customer community. FireEye expertise comes from analysts, experts and incident responders who are constantly scanning for and reacting to the latest

As a trusted security partner, FireEye is uniquely positioned to deliver community protection to you as a member of its customer community.

attacks, geopolitical triggers and cyber events across multiple countries and industries. The company collects machine, victim and attacker intelligence, and quickly codifies and shares it with the community. Based on size, depth and breadth, FireEye has the largest knowledge base of major breaches, attackers, and attack techniques and patterns, and delivers the early detection capabilities that improve protection for every member of the community. As a result, customers in the FireEye community – regardless of industry, size, or geography – know what they should expect and how to respond.

Learn more today at **www.FireEye.com.**

ABOUT FIREEYE

FireEye protects the most valuable assets in the world from those who have them in their sights. Our combination of technology, intelligence, and expertise — reinforced with the most aggressive incident response team — helps eliminate the impact of security breaches. We find and stop attackers at every stage of an incursion. With FireEye, you'll detect attacks as they happen. You'll understand the risk these attacks pose to your most valued assets. And you'll have the resources to quickly respond and resolve security incidents. FireEye has over 4,000 customers across 67 countries, including more than 650 of the Forbes Global 2000.

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

FireEye