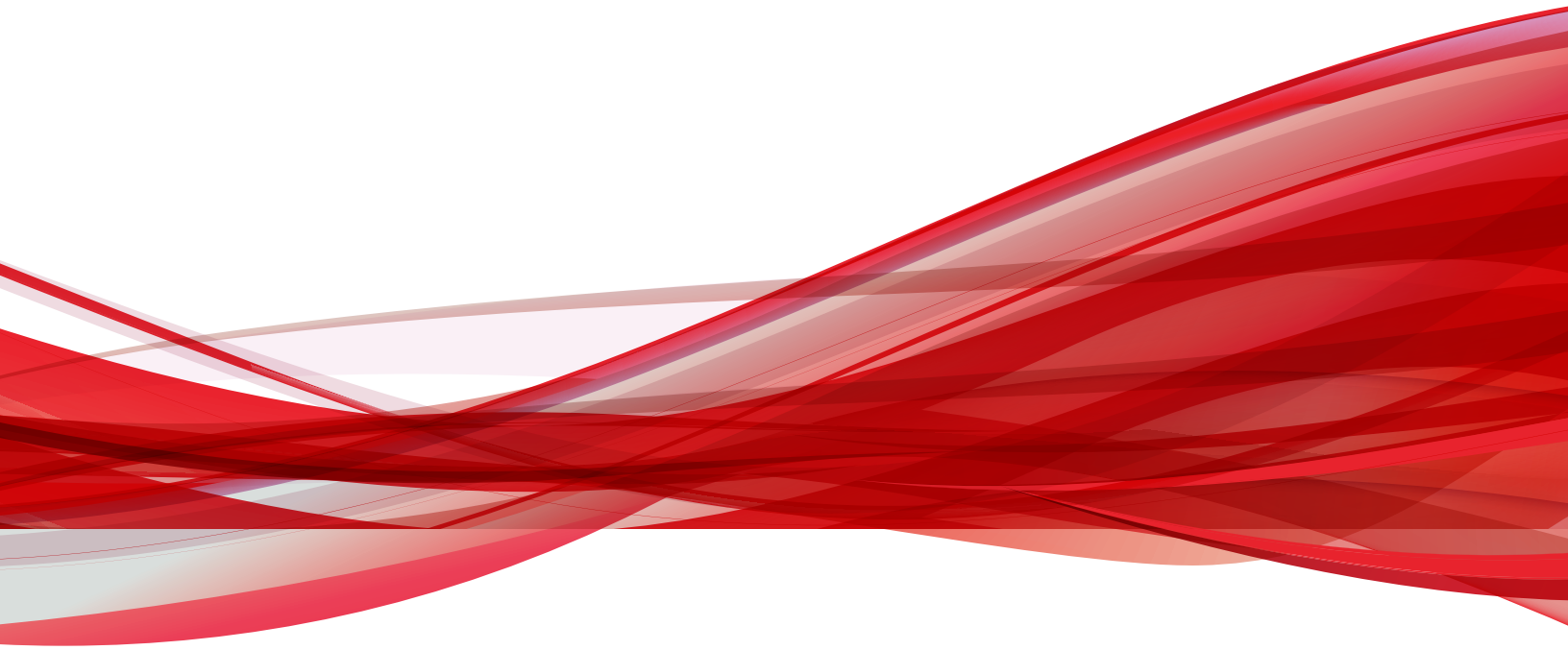
A TREND MICRO WHITE PAPER

A Holistic, Proactive Framework for Identifying and Preventing Cyber Attacks



TREND MICRO™

Securing Your Journey to the Cloud

EXECUTIVE SUMMARY

Cyber criminals have more tools, finances, and technology at their disposal than ever before. Focused attacks on single, high-value targets are increasing sharply. Meanwhile, mobile, wireless, and deeply interconnected online systems create more numerous attack surfaces for threat actors to target and exploit. Founded in 1988, Trend Micro is one of the most experienced and single largest dedicated cyber security provider. The company has delivered over two decades of product innovation to fight cyber crime. Very few cyber security vendors have the multi-million dollar R&D commitment, as many experienced data scientists, and advanced big-data resources that address these threats. Trend Micro remains on the forefront of fighting cyber assaults with its ever-evolving and highly flexible holistic and proactive framework. Trend Micro products have been proven to prevent, detect, and eliminate cyber threats faster than many tested systems in the industry [Source: NSS Labs Consumer EPP SEM Tests 2009, 2010, 2014].

RECENT SINGLE-TARGET, HIGH-VALUE CYBER ATTACKS

From late 2014 through early 2015 the public saw well-publicized cyber attacks on large industrial, government, and private networks. The following are a few representative examples worthy of note due to their high impact and the trends they exhibit. While at first glance they may seem to be wholly unrelated, a number of deeper connections among these attacks are evident after a closer examination.

SONY PICTURES

A few days before Thanksgiving 2014, employees of Sony Pictures who logged onto corporate servers were confronted by an on-screen, red skeleton logo with the text #Hacked by #GOP. Subsequent communiques from the group, identifying itself as "Guardians of Peace," were posted on a hacktivist, text-sharing network called PasteBin, where #GOP posted sensitive internal Sony emails, confidential information on upcoming Sony Pictures releases, and other intellectual property. Sony pulled an upcoming film, *The Interview*, from wide-scale distribution. Hackers also destroyed key portions of Sony server data (see Figure 1).

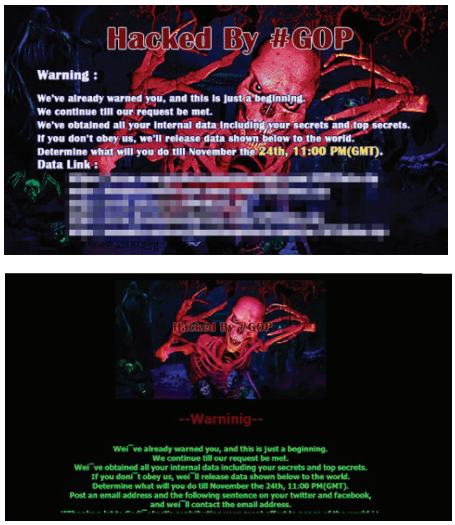


Figure 1: Top: walls.bmp dropped by BKDR_WIPALL.C

Bottom: Scrolling message in an HTML file loaded by BKDR_WIPALL.E

THE U.S. OFFICE OF PERSONNEL MANAGEMENT

On June 4, 2015, officials for the U.S. Office of Personnel Management (OPM) announced that the OPM's data center had been breached—again.[i] Estimates inside the U.S. government admit that up to 22.1 million private personnel files of government employees were compromised, exposing social security numbers, addresses, security clearances, and job assignments. These hacked central repositories of government information contain up to 780 pieces of information on each employee, including spouses and other associates. [ii iii iv]

PREMERA BLUE CROSS

On March 17, 2015, Premera Blue Cross issued a statement that as many as 11 million patient records were accessed and possibly stolen. Suspicious cyber activity at Premera dates back to 2013, when a false web domain was registered: "prennera.com," which may have been used to set up a false web presence.[v] Premera serves primarily government offices and its employees and contractors, and there is some speculation that the information theft was espionage-related.[vi]

TV5 MONDE

In Europe, cyber terrorists claimed responsibility for completely disabling broadcast channels for French public television, TV5 Monde, and posting political material on its social media sites. Cyber criminals claimed that documents they posted on the broadcaster's site were the identity cards of French citizens who are relatives of soldiers stationed in Iraq. In all, 11 channels throughout the worldwide TV5 Monde network went dark for hours. Critical data from TV5 Monde systems was also destroyed.

SINGLE TARGET COMMONALITIES

Common themes among these recent examples include increased sophistication by organized hacker groups; greater resources available to them; and attacks on targets that hold the most sensitive or sought-after data. Increasingly, cyber criminals steal and destroy critical data. Lack of proactive security management, underestimation of the threat landscape, and the increasing complexity of modern networking systems offer highly motivated hacker groups the toehold they need to exploit both private and public networks—from critical infrastructure to government resources. These single-target hacks are not one-size-fits-all, and they require specialized knowledge, skills, and detailed information on the specific target.

ATTACKS BECOME MORE SOPHISTICATED

The threat landscape itself has shifted, with the prime motivations and resources of hackers shaping both the nature of the latest attacks and the targets they pursue (see Figure 2). All forms of cyber crime have evolved dangerously as threat actors use increasingly sophisticated tactics, techniques, and procedures (TTPs), as the following examples reveal:

PAWN STORM

Operation Pawn Storm refers to the economic and political espionage attacks instigated by a group of threat actors primarily targeting military, embassy, and defense contractor personnel from the United States and its allies. Russian dissidents and opposition factions, international media, and even the national security department of a US ally were also targeted. The threat actors used three attack vectors—spear-phishing emails with malicious attachments, an advanced network of phishing websites, and exploits injected into legitimate websites. Secondary infections utilized mobile spyware apps (iOS) to steal information from their victims. As typical in these scenarios, coordinated, multiple threat vectors give the actors a higher infection rate against their victims.

RANSOMWARE

Ransomware is malware that locks a user or users out of their systems until a ransom is paid. In 2013, a particularly vicious form, called CryptoLocker, not only locked up systems but also encrypted all data. Today these forms of attack (CryptoWall and TorrentLocker, e.g.) typically consist of a highly coordinated attack sequence that includes:

Figure 2: Threat actors and their motives.

- Spam runs using numerous socially engineered topics to lure the victim into clicking on a weaponized attachment or an embedded link
- Compromised websites used as either command-and-control (C&C) servers or as redirects to malicious sites
- Captcha webpages to enhance the believability of the attack sequence
- Constantly changing malware to prevent traditional file scanners from detecting threats

These campaigns are being seen across the globe as they are effective and profitable, garnering the threat actors behind them millions of dollars in revenue.

THE GROWTH OF THE CYBER-ARMS BAZAAR

Many of these TTPs for both single-target and widespread attacks are now regularly traded and disseminated over Deep Web sites to a variety of hackers with myriad motives. The underground marketplace for cyber arms technology now offers everything from off-the-shelf hacking tools to made-to-order bots. Cryptocurrency, such as Bitcoin, direct account deposits, and barter are the methods of payment. Transactions are often made through third-party black market intermediaries (called Garants) who vet both sides of the exchange to thwart law enforcement. Motivated individuals and groups can

TREND MICRO EXPERTS TRACK THE DEEP WEB

In its continued effort to thwart cybercrime at its inception, Trend Micro devotes considerable resources in tracking the Deep Web for cyber-criminal activity. Customers can access the latest news on the cyber underground **here**. A few key findings in the latest Trend Micro report, *By the Numbers: the Deep Web*, include the following:

- The going rate for fake U.S. passports on one Dark Web site is $5,900.
- The price for 100 stolen PayPal or eBay accounts on one market is $100.
- Stolen German PayPal accounts with balances of $250-$500 are sold for $100 each.
- Celebrity and political-figure assassination services are solicited online.

Trend Micro keeps close tabs on Deep Web activities in close cooperation with law-enforcement officials. Certain portions of the Dark Web are unreachable by traditional means: yet the dedicated, trained, and highly sophisticated threat researchers at Trend Micro have the expertise to delve into the farthest reaches of this underground to ferret out the latest information on cyber threats and impending attacks. Trend Micro uses this threat actor intelligence to identify new TTPs used by cyber criminals to build better protection for customers.

> "Historically, one had to be a coder, an individual who had to learn to build a cyber-gun and bullet. This is no longer the case. The shadow economy of the Deep Web has become a massive underground marketplace where hundreds of diverse forums produce a myriad of cyber weapons for sale and lease. As a result, criminals are now migrating to cyber crime with ease and are organizing into guilds of thieves who target corporations. This cyber crime wave represents the largest transfer of wealth in world history."
>
> *Tom Kellermann, Trend Micro Chief Cybersecurity Officer*

even contract "hacking-as-a-service" through such intermediaries.

The unfortunate success of this cyber-arms bazaar fuels ever-greater investment and innovation by bad actors and hacking groups. Threat actors now have a growing arsenal of attack methods at their disposal.

FAST, FAKE DOMAINS FOR HACKING COMMAND AND CONTROL

With the broadening and automation of domain name registration, hackers have found a new tool for quickly and easily spawning a large series of rendezvous points for their cyber-attack C&C. Using automated domain name generation algorithms (DGA), thousands of domains can be easily created, and then launched in a matter of minutes, obfuscating the true origination of hacking traffic. Most of the embedded malware on infected systems report to the hacker's C&C servers to receive updates, send captured data from the infected host system, and propagate laterally throughout a host's network, further penetrating and collecting data. On average, in targeted attacks, it takes infected hosts eight months to discover these hidden, slow, and persistent intrusions.

WEAK LINK: HUMAN NATURE

Hackers often rely on human nature itself—the users of network systems—to unwittingly open the doors to valuable data. Personal information, such as interests, known associates, familiar email addresses, or other user-specific data is used to entice users to follow an email-embedded link, click a credible-looking ad, open a weaponized attachment, or visit a fake web site that can immediately download malicious code to compromise the user's system. Once inside the network walls, the attackers spread silently and laterally throughout the business (See Figure 3). Backdoors are introduced to give an outside hacker complete access to systems. From this vantage point, compromised hosts can then receive

further instructions/updates from a masked, outside C&C to dig even deeper into network data centers, or take commands from a live hacker. Once the attackers have found their target data, they then begin to regularly transmit the information to an outside drop zone. In many cases, targeted attacks involve a live hacker accessing files, moving through systems, and unlocking restricted data stores.

WHERE POINT SOLUTIONS FALL SHORT

In the past, with so many vulnerabilities to protect against, companies turned to multiple vendors to upgrade their security status. Where many organizations struggle the most is in integrating these separate point solution products from multiple vendors—any one of which may be in conflict, overlap, or completely miss incoming threats. Many of these point solutions are unable to detect the customized, "low, slow, and masked" attack that is made specifically for the targeted victim. These customized, targeted intrusions do not appear as anomalies to many security software vendors as they have not yet been identified at the time as being associated with other threats found separately within the organization.

Organizations need a holistic system of security in which all security elements communicate seamlessly, sharing information and updates, and above all, a complete picture of all security parameters—inside and out. The old network-security paradigm of reactively patching, fixing, and deploying specific software and hardware for each type of security vulnerability no longer works. In an age of targeted attacks and more sophisticated hacker tools, only a layered and interlocking, continually learning system of security components can provide a framework that gives organizations threat awareness both inside and outside their networks.

"A TIMELINE OF TREND MICRO SECURITY INNOVATION"

Trend Micro has a long history of innovation and industry firsts that often anticipate evolving TTPs. For example, it has been on the forefront of mobile app malware, malicious spam, and the detection of targeted "one-and-done" attacks. These innovations are only possible due to its flexible, continually evolving architecture and significant R&D investments in both technology and highly trained personnel. ***Click here for the full Trend Micro Innovations Timeline.***

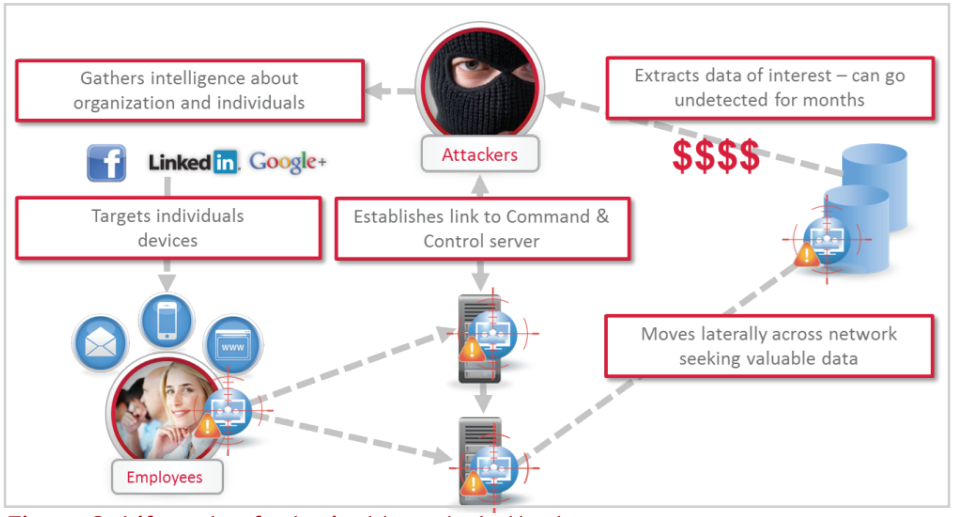


Figure 3: Lifecycle of a typical targeted attack.

HOLISTIC, PROACTIVE FRAMEWORK FOR CYBER THREAT PROTECTION

The best line of defense is approaching network security in a holistic, seamlessly integrated fashion. In this way, organizations are assured that security rules, configurations, and policies are *actively* applied consistently and rigorously throughout the security ecosystem with no conflicts or gaps. Secondly, a *proactive*, predictive framework wrapped around the security environment helps in identifying and isolating potential new and not-yet-identified threats.

This holistic approach requires the following:

- Timely and regularly updated active threat lists
- Monitoring and filtering of incoming/outgoing traffic with advanced analysis
- Port monitoring and management
- Deep inspection of all data on the network
- Use of big-data analytics for retrospective analysis to complement real-time analysis

This internal, coordinated system can then be informed and further strengthened by predictive and proactive analysis of unknown threats. This proactive and predictive layer of protection is more difficult to implement, however. What incoming IP addresses or email constitute a potential threat? How can a security system determine the validity of outgoing data to particular IP destinations?

Examining only one of many threat vectors, over 90% of URLs accessed by Trend Micro customers are already identified and whitelisted

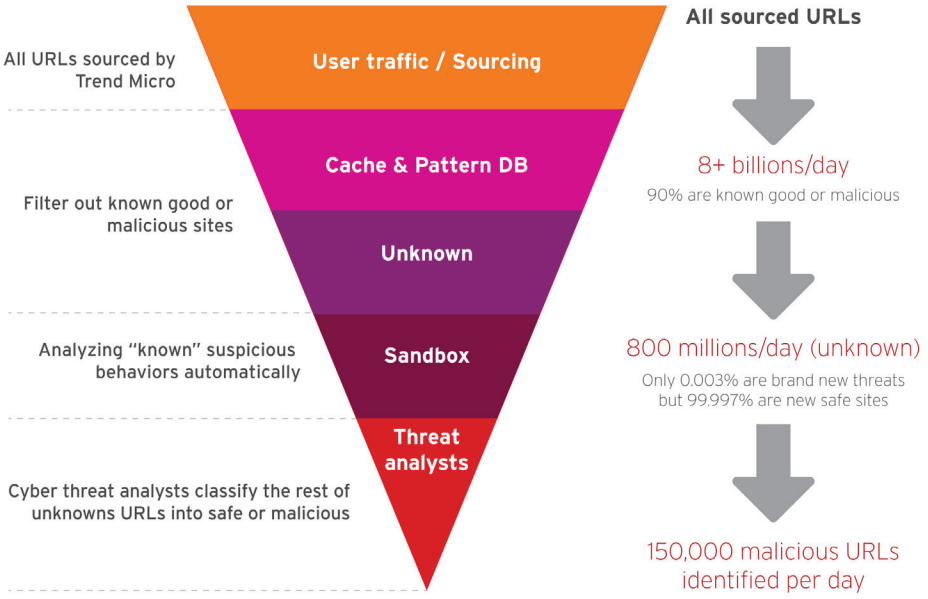


Figure 4: URL-only threat analysis.

(safe) or blacklisted (malicious) by reputation-management databases, from both externally trusted sources and internal lists maintained by Trend Micro (see Figure 4). This means that over 800 million URLs may be unsafe sites, with more being spawned every day. Approximately 150,000 sites are identified as malicious on any given day, but scanning 800 million sites each day is a challenging proposition.[1]

Using sophisticated big data analytics, data scientists at Trend Micro can determine which new domains, IPs, URLs, files, mobile apps, and other suspicious samples should be subjected to further scrutiny. If obvious security anomalies are shown in the automated testing, they can be immediately blacklisted. Many others will be found innocuous and safe, and these will be whitelisted. A percentage may not show definitive results one way or the other, however, and must be turned over to expert data scientists for evaluation.

Big-data analysis using both automation and human inspection on a 24x7x365 basis due to the global, non-stop nature of new threats

Using sophisticated big-data analytics, data scientists at Trend Micro can determine which new domains, IPs, URLs, files, mobile apps, and other suspicious samples should be subjected to further scrutiny.

requires resources that most security software companies do not have the capital or human resources to address. Trend Micro, however, uses this proactive intervention as one element in effective prevention of the latest cyber threats. Big-data is only as good as the data collected, as well as the analysts who use it, and who understand the core principles of various attack vectors. This experience cannot be fully automated nor programmed into discrete software modules. Once threats are identified—or cleared—by data scientists, these previously unknown threats can be entered into live updates and distributed to the integrated security systems at customer sites.

[1]All figures are derived from internal Trend Micro historical and current research, development, and monitoring.

TREND MICRO GLOBAL THREAT DATA

Trend Micro continues to evolve and improve its entire ecosystem of integrated security products. At the heart of its layered and continually evolving threat detection is the Trend Micro™ Smart Protection Network™ global threat intelligence system. This proactive cyber security monitoring platform feeds predictive, actionable intelligence into all Trend Micro product solutions including email filtering, network traffic monitoring, C&C communications, malware detection, and deep data inspection. Released in 2008 after four years of intensive research and development, the Smart Protection Network is continually evolving and adapting to the changing nature of the cyber-threat landscape today (see Figure 5).

The Smart Protection Network includes, but is not limited to the following:

- Hundreds of millions of sensors across the globe
- Heuristic machine learning of threat vectors
- Continuous big-data global analysis
- Cloud-based Hadoop for high volume data processing
- File analysis
- Pattern recognition to identify suspicious outbound traffic
- Filtering of unknown URLs, attachments, and mobile apps

With over 500,000 corporations, agencies, and business installations and tens of millions of consumer customers, Trend Micro has an enormous base of real-world knowledge and experience to draw upon. Few, if any, security vendors have these reporting and monitoring capabilities to continually improve their product lines. More important,

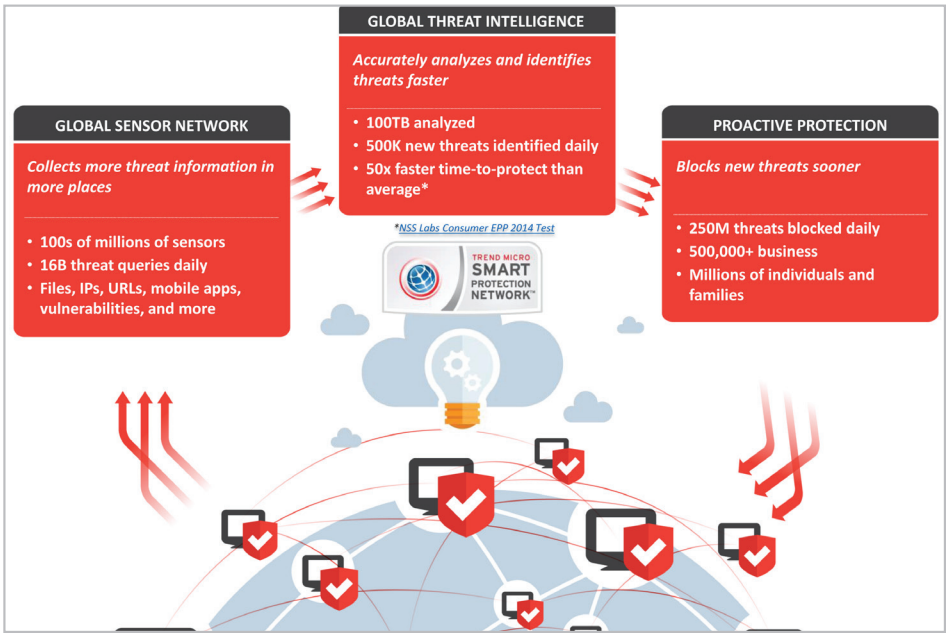


*Figure 5: Sensing and tracking of all cyber-threats in real-time with the Trend Micro Smart Protection Network. [*NSS Labs 2014 Consumer EPP SEM test.]*

this vast installed base serves as a source of tremendous actionable intelligence and a daily proving ground for further improving Trend Micro technology. This data collection network (Global Sensor Network) is supported across many layers of the network. The Smart Protection Network is integrated into all Trend Micro solutions including mobile, endpoint devices, servers, networks, messaging, gateways, and cloud-based SaaS solutions to collect threat data wherever the threat is introduced or has moved.

With the data from its global sensors, the Smart Protection Network hands off threat queries to its threat intelligence infrastructure, where anomalies (such as attachments and executable attached code) and newly born domains are first checked against reputation management databases and internal Trend Micro threat lists. Next, big-data analytics are applied to threat candidates to determine any suspicious patterns or behavior. Big-data visualization techniques are useful, for example, in finding live, malicious C&C centers. Figure 6 shows that a specific endpoint was assigned a number

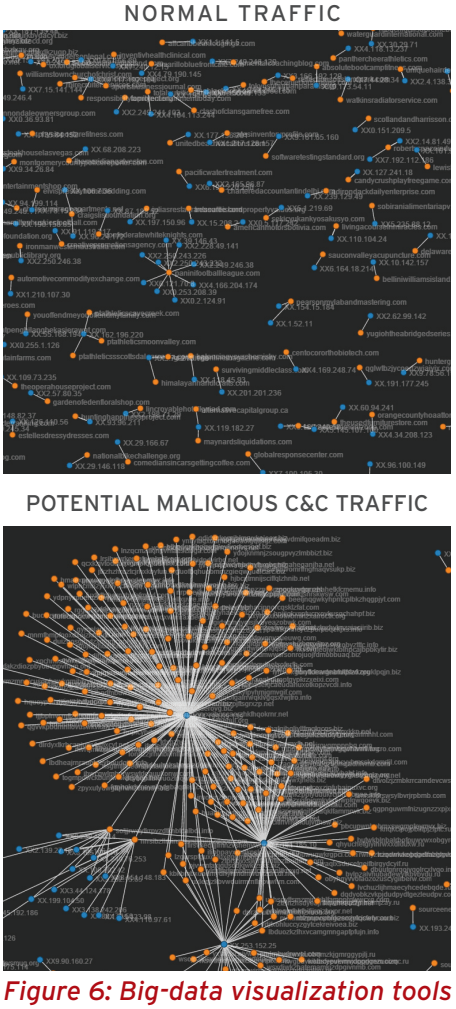


Figure 6: Big-data visualization tools to find suspicious C&C patterns in Internet traffic.

"BETTER TOGETHER" SECURITY

Trend Micro's use of isolated testing sandboxes for suspicious files, domain originations, and file attachments enables its worldwide, cloud-based network to quickly test out any and all potential threats. Customers can now deploy similar technology (Trend Micro™Deep Discovery ™) within their own premises, particularly those threats that may be specifically targeting their organization. This on-site sandbox testing provides even faster collection, detection, and protection with no risk to the overall network. On-site customized sandboxes are also in touch with the Trend Micro cloud, sharing and distributing threat warnings as they are discovered. Inside and outside new threat live testing is the best of both proactive tactics, delivering a community of threat detection environments that benefit all with "better together security."

of newly born domains in a short period of time, making them highly suspicious, and candidates for further analysis.

These suspicious URLs, mobile apps, attachments, or other executable code can be forensically examined in safe, isolated Trend Micro sandbox environments where software and analysts can observe their actions when executed. Finally, if an uncategorized, unknown potential threat is still not definitively deemed safe, it is turned over to data scientists who can perform further meta-analysis before making a final determination.

An important function of the Smart Protection Network is its ability to learn from its former actions: patterns of newly identified threats are maintained (sometimes for years) in the growing dataset of the Smart

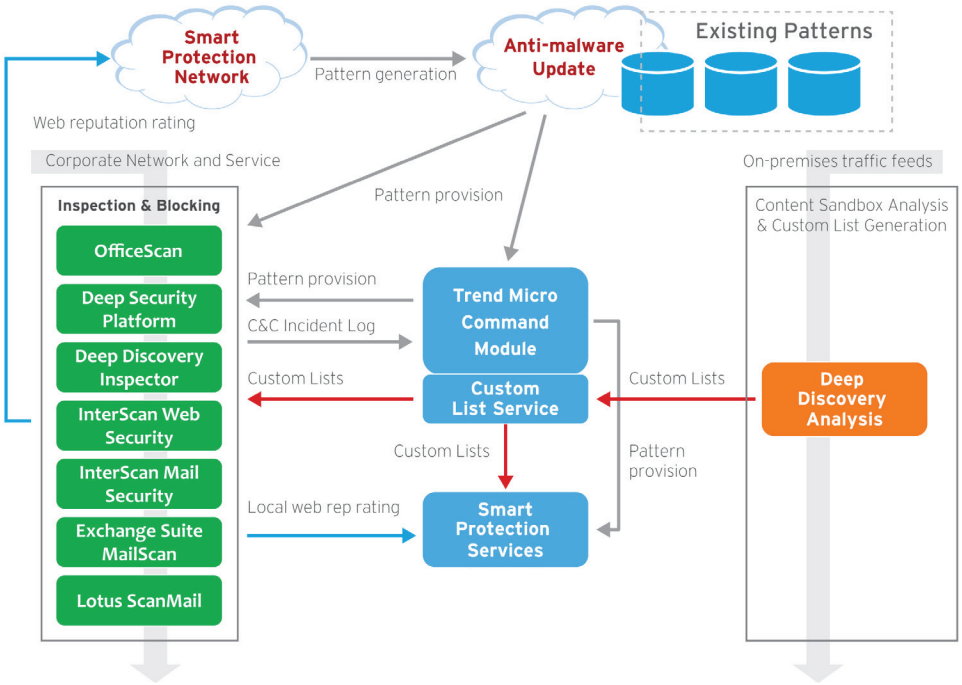


Figure 7: The innovative, holistic security framework of integrated Trend Micro products.

Protection Network for use in the future (i.e. retrospective analysis). Trends associated with customer type, geolocation, industry, and other metadata are identified and included in this historical information. In addition, any threats detected at installed Trend Micro customer sites are immediately forwarded to the Smart Protection Network, where they are compared to known threats and catalogued. All of this near-real-time, actionable intelligence is then distributed through the Trend Micro cloud to update all its solutions and services around the clock to its worldwide customer base.

Trend Micro big data innovation does not end at the customer network edge, however. Analytic engines embedded in Trend Micro security software and appliances also monitor outgoing traffic from customer sites. Traffic patterns are accumulated and any suspicious outbound traffic is examined, again by analyzing URLs/domains/IPs to potential hacker C&C servers or drop zones. In this way, potential malicious communications that were once dormant can be isolated, analyzed, and neutralized even if new malware is somehow introduced into the host network. Meanwhile, Trend Micro antimalware and deep data inspections also search out malicious threats that may be on the network or any of its endpoints. These elements work in tandem, around the clock, to provide a proactive, holistic approach to cyber threats (see Figure 7).

TREND MICRO ADVANTAGES

Using its holistic framework as a complete, integrated global threat intelligence platform, Trend Micro delivers innovations and best-of-class services not found in other, stand-alone security products.

CONNECTED THREAT DEFENSE

To adequately protect against the current threat landscape, you need to implement a full life cycle of threat defense. The life cycle of threat defense consists of four stages: **Prevent**, **Detect**, **Analyze**, and **Respond**. Each of these stages uses a series of techniques to keep you protected.

- Prevent: proactively protect servers, endpoints, applications, and data are from identified threats.
- Detect: detect advanced malware, malicious behavior, and communications that are invisible to standard prevention techniques.
- Analyze: assess the risks and nature of attacks, including retrospective analysis to determine the impact of these threats.
- Respond: deliver real-time signatures and security updates to recover from past attacks and prevent future attacks.

For the best possible security posture, there must be connections between the stages of the life cycle. This connected threat defense ensures that threat intelligence gained by techniques in one stage is automatically and rapidly shared with the other stages.

A connected threat defense delivered through a fully integrated solution also facilitates central visibility and control, delivering a connected threat defense with a complete view of all users and network security. Plus, it makes it simpler for organizations to investigate threats and to administer day-to-day management.

MOBILE APP REPUTATION

Trend Micro developed and continues to improve the industry's first mobile app reputation management system. It dynamically collects and rates mobile apps based on malicious activity, resources used, and potential privacy and security vulnerabilities.

CLOUD-BASED WHITELISTING

As a leader in cloud-based, highly responsive analysis of traffic, Trend Micro leverages one of the world's largest databases of "good" files and applications (GRID – Goodware Resource and Information Database). This dramatically reduces false positives and enables Trend Micro's dedicated data scientists to focus more resources on new potential threats.

VULNERABILITY RESEARCH TO STOP EARLY THREATS

As the most experienced security-only developer, Trend Micro has long-standing relationships with all leading software and network component vendors. As a result, vulnerabilities and potential exploits are often caught and remediated well before hackers even know they exist. In addition, Trend Micro Vulnerability Research is at the forefront in detecting mobile and smartphone threats. As a result of this effort, its proactive approach regularly finds and thwarts zero-day exploits and virtually patches known vulnerabilities.

NETWORK TRAFFIC INTELLIGENCE, BIG DATA-MINING CORRELATION

Trend Micro is a leader in collecting and analyzing network traffic—with both rules-based, machine-learning tools, and a team of experienced data scientists. This coordination of efforts—both machine and human analysis—not only discovers individual botnet and other single attacks but also correlates seemingly unconnected traffic patterns to discover multi-vector threats. This analysis is a 24x7x365 operation that sifts through gigabytes of data every hour. Trend Micro data scientists also perform proactive penetration testing to identify vulnerabilities before any hacker can.

THREAT ACTOR INTELLIGENCE

Trend Micro, in cooperation with law enforcement, actively monitors the Deep Web and hacker marketplaces to uncover new hacker tools, attack vectors, and even targeted attacks to protect against them before they are launched.

ENHANCED WEB, EMAIL, AND FILE REPUTATION

Trend Micro maintains one of the world's largest web reputation databases. Sites are scored on age, location changes, and suspicious behavior. Through a two-tier system, Trend Micro examines both single and multi-component testing of web sites, sandboxing and testing of new components on existing sites, and monitoring of cyber-criminal activity. Real-time page analysis, using script analyzers and browser exploit prevention technology, identifies new malicious URLs at the time of access. The result is industry-leading blocking of both existing and evolving threats to Trend Micro's customers.

Trend Micro's enhanced email filtering technology combines domain reputation, content analysis, and back-end, rules-based data correlation to identify email threats in real time—especially those not already on threat warning lists. (See the following section: Trend Micro Email Filtering.)

As a leader in cloud-based detection and protection, Trend Micro intercepts attachments or file downloads before they are delivered to a system, caching and comparing files against Trend Micro community file reputation databases and leading reputation databases that ID suspicious files based on metadata, prevalence, geolocation, and other signs of malicious behavior. Suspect files are immediately analyzed. The entire process is fast and thorough, and it does not impede legitimate file exchanges.

SMART PROTECTION SERVER

Smart Protection Server is an on-premises solution for companies that want the bandwidth and privacy

advantages of on-site analysis and queries of suspect URLs, email, and files. This solution provides all the protection of the Trend Micro cloud-based service yet preserves bandwidth and privacy.

SMART FEEDBACK

Any time a single, targeted attack is identified on any Trend Micro-protected customer site, the attack is signaled to the 24x7 "neighborhood watch" system consisting of all Trend Micro customers. In this way, each and every Trend Micro site can inform and protect the entire community, improving the speed with which new threats can be identified and stopped. Customers can opt in within the supported solution's admin console and include their industry categorization.

INDEPENDENTLY TESTED, AWARD-WINNING PROTECTION

This holistic, proactive framework of Trend Micro security has a proven track record in the field that is borne out in independent lab testing. In a 2015 AV-TEST Labs examination of leading security products, Trend Micro provided 100% protection against both zero-day and widespread malware, versus the industry averages of 96% and 98%, respectively. In AV-Comparatives Real-World Protection test (Mar-Jun 2015) Trend Micro achieved a 99.7% real-world test score versus the industry average of 97.1%. Trend Micro Deep Discovery was rated the most effective 'Recommended' breach detection system in 2015 NSS Labs testing.

Trend Micro's continual innovation has not gone unnoticed. *Network World*, one of the oldest and most respected IT publications, tested Trend Micro™ Premium Security in its independent labs against the leading competitors and declared Trend Micro its "2015 Clear Choice Winner" in its anti-virus category. Read more about Trend Micro independent testing **here**.

Domain	Time Lapse Between Registration and Spam Activity
bu_____b.com	0:02:44
fu___k.com	0:02:45
van_____f.net	0:04:36
bo__z.net	0:04:57
to_____b.net	0:05:03
ya___g.net	0:05:05
ab_____s.net	0:05:10
ag___b.net	0:05:14
ro___y.net	0:05:14
fa_____s.com	0:05:29
op____w.com	0:07:12
to____g.com	0:13:35

Figure 8: Time lapse between creation of new malicious domains and their first outbound attacks.

EXAMPLE: TREND MICRO EMAIL FILTERING

The way in which Trend Micro filters and protects email is an illustration of the integrated and proactive nature of its entire product line.

Hacker groups can deploy newly born domains and launch spam campaigns in a matter of minutes (see Figure 8). They can then launch phishing attacks that lure users to click on links to seemingly legitimate web sites or open attachments from purportedly trusted sources. These newly born domains escape many normal threat detection systems. With the Smart Protection Network as the first line of defense, these messages can be outright blocked due to suspect domain analysis using automated controls. This advanced filtering technology works hand-in-hand with Trend Micro™ InterScan™ Message Security software and virtual appliance, Trend Micro™ Hosted Email Security, and ScanMail™ for Microsoft Exchange™.

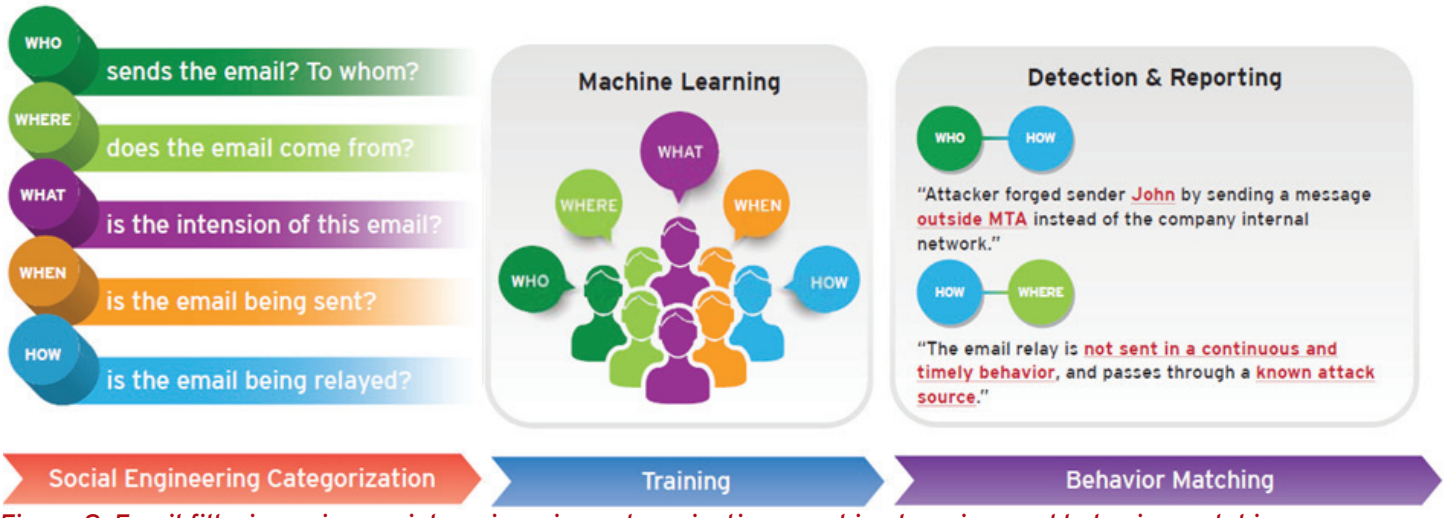


Figure 9. Email filtering using social-engineering categorization, machine learning, and behavior matching.

Trend Micro™ Social Engineering Attack Protection inspects the behavior of emails not only by their origination, but also by examining key characteristics of each email: *who*, *what*, *when*, *where*, *why*, and *how*. Attack Protection follows a set of actions:

- **Social engineering** categorization: Distinct social engineering behaviors displayed within email are categorized into a features list, which is used to identify targeted attack emails.
- **Training:** The features list is fed into a set of correlation combinations, each of which represents social engineering scenarios that are known to represent attack methods.
- **Behavior matching:** The correlation combinations are the core basis for identifying targeted attacks. After an email is detected as a possible attack venue, an analysis report is generated that details why the email is suspect based on the five core social engineering criteria of who, what, where, when, and how.

Positives are isolated immediately, and potential threats are forwarded for further examination while genuine emails are passed along (see Figure 9). All of this happens in the background and is fed and evolves continually using real-time data from the Smart Protection Network. Trend Micro antimalware, document and file scanning, and IP traffic monitoring employ similar holistic, predictive processes through module software, appliances, and actionable intelligence provided by the global Smart Protection Network infrastructure.

CONCLUSION

Trend Micro is one of the largest developers of software devoted exclusively to the cyber security of computers, networks, and network-attached devices. Its Smart Protection Network infrastructure works hand-in-hand with its customer-based software products and security appliances. A unique combination of global Internet big-data analytics managed by experienced data scientists is used to populate customer-based Trend Micro systems with threat warnings much earlier than other security solutions. In addition, the holistic framework of the Trend Micro platform delivers a seamless internal security environment that also monitors and isolates any suspicious outbound communications. In this way, Trend Micro not only protects systems against a wider array of threats but also can more easily and proactively identify targeted, custom-made attacks.

Trend Micro, through years of expertise, continuous innovation, and unmatched global R&D resources delivers the following unique and unrivaled assets in the ever-evolving fight against cyber threats:

- One of the most advanced, cloud-based big-data security analytics engines
- A large team of data scientists devoted exclusively to cyber-threat detection and prevention
- A holistic, "no gaps" proactive and tightly integrated security platform

Trend Micro has over 500,000 corporations, agencies, and business installations and tens of millions of consumer customers for ongoing intelligence as a basis for continual product improvement and technology innovation.

REFERENCES

[i] Bennett and Diersing. "Hacked federal files couldn't be encrypted because government computers are too old." LA Times. June 10, 2015. **http://www.latimes.com/nation/la-na-government-data-breach-20150616-story.html**

[ii] Levine, Mark. "OPM Hack Far Deeper Than Publicly Acknowledged, Went Undetected For More Than A Year, Sources Say." ABC News. June 11, 2015. The Guardian. "Second hack of federal records hit intelligence and military personnel." June 12, 2015. **http://www.theguardian.com/technology/2015/jun/12/hacking-personnel-data-4-million-federal-workers**

[iii] Levine, Mark. "OPM Hack Far Deeper Than Publicly Acknowledged: Went Undetected For More Than A Year, Sources Say." ABC News. June 11, 2015.

[iv] Nakashima. Washington Post. July 9, 2015. **http://www.washingtonpost.com/blogs/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/**

[v] Shahani, Aarti. "Premera Blue Cross Cyberattack Exposed Millions of Customer Records." National Public Radio. March 18, 2015. **http://www.npr.org/sections/alltechconsidered/2015/03/18/393868160/premera-blue-cross-cyberattack-exposed-millions-of-customer-records**

[vi] Finkle, Jim. "Premera Blue Cross breached, medical information exposed." Reuters. March 17, 2015. **http://www.reuters.com/article/2015/03/18/us-cyberattack-premera-idUSKBN0MD2FF20150318**

[vii] Network World. "2015 Clear Choice Winner: Antivirus." **http://cloudsecurity.trendmicro.com/us/technology-innovation/awards-reviews/index.html#product-awards**

TREND MICRO™

Securing Your Journey to the Cloud