BLURRING BOUNDARIES

Trend Micro Security Predictions for 2014 and Beyond
PREDICTIONS

1. Mobile banking will suffer from more MitM attacks; basic two-step verification will no longer be sufficient.

2. Cybercriminals will increasingly use targeted-attack-type methodologies like open source research and highly customized spear phishing, along with multiple exploits.

3. In the context of targeted attacks, we will see more clickjacking and watering hole attacks, new exploits of choice, and attacks via mobile devices.

4. We will see one major data breach incident a month.

5. Attacks leveraging vulnerabilities in widely used but unsupported software like Java 6 and Windows XP will intensify.

6. The Deep Web will significantly challenge law enforcement, as the latter struggles to build capacity in order to address cybercrime on a large scale.

7. Public distrust will ensue, especially after the exposure of state-sponsored monitoring activities, resulting in a period of disparate efforts to restore privacy.

8. We will not yet see large-scale, widespread IoE threats. This requires a “killer app,” which may appear in the area of AR in the form of technology like heads-up displays.
Last September, Trend Micro partnered with Europol and the International Cyber Security Protection Alliance (ICSPA) to release “2020: The Series” and its accompanying paper, which show how technology could be used and subverted in the future.

If you read the paper or watched the episodes, you’ll see how 2020 could usher in the integration of many interesting technologies with each individual, organization, and even a nation’s existence. By then, most people would use heads-up display (HUD) glasses and maybe even contact lenses that respond to hand gestures every day. Each netizen will enjoy highly personalized online content, thanks to continuous data monitoring and gathering through sensors or implants. Smart grids will run basic services and aid technology-assisted living; fully automated government elections will become a reality. Conversely, new threats and cybercrime types will emerge; some can even destroy critical infrastructure and cause physical injury.

In the “2020: The Series” episodes, we tried to visualize what will likely come true and came up with a lot of scenarios that you may not immediately see. Guess why the cybercriminals wore HUD contact lenses while the law enforcers wore HUD glasses. Because the contact lenses are powered by a biochemical reaction and you need a new pair every day. That can be expensive! How did the police get video evidence out of one of the main character’s bedroom? I just presented on smart TV hacking at the RSA Conference in Europe, that should give you an idea. You can also watch “2020: The Series”, which has references to “Blade Runner,” one of my favorite movies of all time, to find out.

Will these future scenarios see the light of day? Interestingly enough, their seeds have been sown and we’ll continue to see them grow in the near future. 2013 played host to major mobile threats, a trend we’ll continue to see in 2014. Mobile devices will become the attack vector of choice, bringing in nastier threats and attacks; basic two-step verification will no longer be sufficient. The line dividing cyber and targeted attacks will blur, as cybercriminals adopt methodologies more identified with targeted attack campaigns. Attackers, whether cyber or targeted, will continue the search for new exploits of choice and use reliable and easily obtainable exploits to get what they want. Law enforcement agencies will step up but face new challenges in the form of unknown territory—the Deep Web—and public distrust caused by revelations of state-sponsored monitoring.

The “Internet of everything” (IoE) is still a buzzword though. The wait for the so-called “killer app,” that one app or device that will change the landscape as we know it, will continue. Only until it gains enough mass is it likely to warrant attacks against it. Google Glass and smart watches have made headlines this year, so we expect competing “wearable” technologies to crop up soon. Smart meters have either been or will soon be rolled out. Research on attacks against industrial control systems (ICS) and tracking technologies like the Automatic Identification System (AIS) have piqued public interest. We’re bound to see more proofs of concept (PoCs) but will continue to stay at the forefront of emerging trends and technologies and be ready to combat the threats they bring.

Before taking on future threats though, let’s focus on the here and now, and prepare for what’s up ahead. One of my private email addresses was found in the recently leaked Adobe database. And guess what, I started getting a lot of spear-phishing emails in my inbox. Fortunately, years of working in the security industry has made me paranoid and extremely careful that I analyze even legitimate-looking emails before opening them. You should too. Be very careful and stay safe in 2014 and know that it helps to be a little paranoid when it comes to computer security!

Raimund Genes, CTO
The past year saw a notable surge in online banking threats. The third quarter saw the infection count pass the 200,000 mark, the highest it has ever been.

But banking threats were not limited to computers; we also saw them go mobile. Fake banking apps became a common problem. Banking-related apps also became a favored cybercriminal target, led by malicious apps posing as token generators.

Going mobile unintentionally rendered two-step verification insufficient. As more people used mobile devices for both banking and authentication, cybercriminals started intercepting authentication numbers with the aid of mobile malware like PERKEL and ZITMO.

Nearly one in five U.S. smartphone users banked via mobile devices in 2013, a number that is expected to rise more in the coming years. 2014 will be about mobile banking. Unfortunately, we can also expect mobile threats like man-in-the-middle (MitM) attacks to increase in 2014.

Android™ will remain the most dominant OS in the market. But this dominance will continue to be exploited, as we predict the volume of malicious and high-risk Android apps to reach 3 million by the end of 2014. Though Google did exert effort to address this, most recently with the release of Android KitKat, not all users can take advantage of new security features due to the OS’s heavily fragmented update process.

New OSs like Tizen, Sailfish, and Firefox that boast of having an Android-compatibility layer will enter the mobile market. On the upside, this layer will allow Android apps to run on the OSs but may also make it easier for cybercriminals to create multiplatform threats.
Cybercriminals and threat actors or those behind targeted attacks typically “share” tools of the trade. Apart from motive though, the way by which they execute attacks differ. Targeted attacks are characterized by persistence and stealth—factors required for data exfiltration.

This year, the Safe campaign obtained 12,000 unique IP addresses spread over more than 100 countries using only two sets of command-and-control (C&C) server infrastructure, proving that size doesn’t matter. Even the smallest attacks can work against the biggest targets. Safe and similar campaigns’ “success” have convinced cybercriminals to adopt targeted attack techniques.

More recent reports also revealed that around 150 samples that can take advantage of the newly discovered Microsoft zero-day vulnerability (CVE-2013-3906) have been found, making it a likely candidate for exploit of choice in 2014.

In 2014, cybercriminals will increasingly use targeted-attack-type methodologies. Doing open source research and spear phishing will become a norm even for cybercriminals.

The “allure” of targeted attack techniques goes beyond campaigns’ success rate though. They will also be adopted because of ease of use and effectiveness in terms of evading detection. Spear phishing is relatively easy to do; creating malware using reliable exploits only takes a few minutes; and, best of all, lateral movement typical of targeted attacks makes their components harder to track.

Vulnerabilities, particularly CVE-2012-0158 and CVE-2010-3333, will continue to be heavily favored not just by threat actors, but by cybercriminals as well, because of their proven track records. CVE-2010-3333, for instance, was the most exploited Microsoft® Word® bug until CVE-2012-0158 came along.

Note though that cybercriminals will not just rely on weak spots in software and systems. In true threat actor fashion, they will continue go after the weakest link—humans.
This year, Facebook fell prey to a watering hole attack; the culprit—an iPhone® developer site. This attack was notable due to its preciseness and the victim's significance; the attackers infected a page they knew would attract their desired target. This incident showed the industry that threat actors need not rely on traditional email-and-attachment tactics to successfully launch attacks.

We will see more watering hole attacks in 2014. Threat actors will lure targets to a watering hole site using a clever social engineering ruse or clickjacking in order to compromise computers with exploits.

The latest Internet Explorer® zero-day exploit (CVE 2013-3918) will become threat actors' trump card. It was already used in an attack that ironically targeted individuals interested in “national and international security policy.”

With fewer OS vulnerabilities found, threat actors will instead focus on bugs in certain software suites. Special attention will be given to those that will no longer receive vendor support, leading to more attacks targeting newly discovered vulnerabilities.

Threat actors will not solely rely on email as attack vector of choice. With the steady rise of consumerization in the workplace, mobile devices will increasingly become the attack vector of choice. Threat actors will target any device to get in to their target networks. This means that wearable devices like smart watches will also become new targets. Any device can and will be used to get in to target networks.
Data remains a top prize for both cybercriminals and threat actors. The recent Adobe breach compromised an estimated 150 million accounts. It has since triggered a domino effect; other service vendors warned users to update their accounts in the off-chance they used the same log-in credentials.

2013 was marked by several data breaches. Evernote asked its 50 million users to reset their log-in credentials after discovering that hackers could have gained access to their information. The LivingSocial breach exposed the credentials of 50 million users while the Yahoo! Japan incident leaked 22 million user IDs to the public.

Major incidents like these will continue to ensue in the coming year. Web servers like those involved in the Adobe breach will continue to be targeted. No organization will be safe from data breaches. Someone will always attempt to break in to networks using new tools and by exploiting vulnerabilities.

Stolen data will be “cleaned up” or dissected into better-quality chunks (i.e., more customized or targeted) before being sold underground. For instance, instead of posting an entire list in public locations, cybercriminals will chop data up not only by region but also by gender or income bracket, depending on what type of information is available. We will thus see new and more “creative” ways to monetize stolen data, which will lead to a more competitive cybercriminal market.
Cybercriminals and threat actors always look for “cracks” in security to initiate attacks. The end of support for Java 6 earlier this year proved to be a golden opportunity.

An active exploit that targets an unpatched vulnerability in the software soon found its way into the wild. The said exploit was then integrated into the Neutrino Exploit Kit, which is known for infecting computers with ransomware. What made the attack more troubling though was that a good number of Java users—around 50%—still used Java 6.

Cybercriminals often reverse-engineer released patches to check which flaws have been addressed and use that knowledge to target older, especially unsupported, software. This may have been the case for Java 6 attacks.

Bad guys also exploited vulnerabilities in specialized software. Vulnerabilities in Adobe® ColdFusion®, normally used in Web application development, were repeatedly exploited to infiltrate databases. This year alone saw massive data breaches targeting several military, government, and space research agencies, reportedly effects of gaining illegal access to the ColdFusion source code.

As Microsoft officially ends support for Windows XP in 2014, we will see the Java 6 scenario play out for the former as well. Expect a pickup in attacks, zero-days, and exploit integration into known kits, among other things. This is alarming given that computers running the OS are six times more likely to be infected compared with other Windows versions. The number could only increase once support stops.

Data suggests that around 20% of PC users still run Windows XP. While the number may not be as big as the Windows 7 base, they still represent a good number of potential victims. It doesn’t help that Windows XP still has a current install base of over 300 million computers inside corporations as well.

Embedded systems, including point-of-sale (PoS) terminals, healthcare devices, and critical infrastructure, may also pose network threats, as they often run older and unsupported Windows versions. While they may be highly specific, cybercriminals will take advantage of the lack of support and use them as points of entry.

Expect ColdFusion attacks to continue in 2014 as well because the recent ones revealed many “high-value” victims. Cybercriminals will continue to launch similar attacks in hopes of netting other high-profile targets.
The Deep Web was momentarily thrust into the spotlight with the Federal Bureau of Investigation (FBI) seizure of the underground marketplace, Silk Road. But that was deemed a minor victory, as a new version of the site was spotted a month after the takedown. Other marketplaces soon followed, boasting of “better security” for merchants and buyers alike.

Addressing cybercrime is difficult because its nature inherently differs from “regular” crime. Law enforcement agencies may not have the correct protocol or personnel to handle cybercrime. Complications also arise when investigations involve different states and countries, which have varied sets of laws and protocols.

Cybercriminals will go “deeper” underground next year. The Deep Web offers anonymity through “darknets,” a class of networks that guarantee anonymous and untraceable access. The most popular darknet is The Onion Router (TOR), which hides a shared file’s origin and destination. The Deep Web also allows cybercriminal content to evade detection by “escaping” search engine crawling. Content posted on the Deep Web is not accessible through the public Internet infrastructure.

Law enforcement agencies, which may not have enough knowledge or experience to deal with cybercrime, will have a harder time tracking criminals in the Deep Web. These underground developments will prompt law enforcement agencies to invest more to fight cybercrime. We will see more initiatives from international organizations, led by developed countries, which are becoming more aware of the situation and taking concrete action. They are bringing in experts to train their law enforcement agents. Unfortunately, third-world countries are 4–5 years behind.
Classified documents obtained by former National Security Agency (NSA) contractor, Edward Snowden, highlighted the perplexing position of privacy within the digital age.

Spyware use is no longer limited to cybercrime. Spyware have, in fact, made their way to governments’ hands for political espionage. We even see spyware sold commercially, often marketed as a means to “track” cheating partners or spouses. The mainstream use of spyware—and the act of spying—has blurred the line between information that's “private” and “public.”

Privacy concerns are driving users to be more aware of their presence in the digital space. Teenagers are leaving Facebook for messaging apps. With over 1.2 billion monthly active Facebook users, teenagers are finding little privacy within the social network. They instead rely on messaging apps for more personal and social interactions. Among these, WeChat saw the greatest growth—a 1,021% increase in its active user base, aged 16–19. Photo-sharing app, Snapchat, meanwhile, boasted of 350 million “snaps” or images sent daily. The large number could be due to the auto-delete function of the app that offers a way to protect a user's privacy.

The exposure of state-sponsored monitoring will push entities to reconsider where they choose to store their data. Distrust in using U.S. infrastructure may ensue, with foreign governments possibly discontinuing their use. Concerns over international monitoring may cause some states to consider revising policies, specifically those involving Internet use. Despite public outcry though, we will see more of these types of state-level monitoring to occur.

Amid privacy concerns, cloud service providers will have to continue showing security controls and data privacy protection. We will see more of them team up with third-party security companies to ensure data protection and privacy. This will give rise to the bring-your-own-controls (BYOC) trend, which will allow customers to make sure data is segmented, protected, and unreadable to unauthorized parties.

Users will realize that to keep their privacy, they will have to control who sees their information, regardless of motive. They will more conscientiously safeguard their privacy on major sites like Google and Facebook. They will exert effort to learn more about tools that will help them protect their data and control what they share online. They may even consider exploring underground encryption tools like TOR to ensure that their information remains private.

We will see more companies profit from selling data for advertising purposes. Big data mining companies will continue to flourish.

Business will remain the same for cybercriminals. They will continue to monetize stolen data, thriving in underground markets.
As more devices become interconnected, securing them means protecting all access points, including the Internet.

**SCADA SYSTEM IMPROVEMENTS**

Past research and PoCs showed that supervisory control and data acquisition (SCADA) systems often remained lacking in terms of security. Efforts are now being made to address this. Bug bounty programs have been established and vendors now have teams exclusively created to ensure SCADA security. But despite security limitations, SCADA system implementation continues. Italy has rolled out smart meters; the rest of Europe will soon follow suit.

PoC attacks on SCADA networks will continue. These attacks, along with more discussions and research, will show just how flawed SCADA networks are when it comes to security. SCADA networks often rely on physical isolation as security defense, making it all too easy for attackers to target them.

**THE NEW EASY TARGET**

Radio-frequency-enabled technologies, meanwhile, will become the new “easy target” of PoC attacks. Often used in tracking technologies like the AIS, radio frequencies will become a new attack entry point. And because AIS is used for maritime traffic and coordinating passenger ships and commercial (i.e., nonfishing) ships, such a vulnerable system could soon be exploited by malicious individuals.

**GAMERS ARE THE NEW BIG FISH**

Other Internet-facing devices will become popular targets as well. The introduction of the Steam Machine and the Linux-based SteamOS will cause major changes in gaming threats. The popularity of the console will dictate if gaming malware will adapt to widen their target base.

The allure of targeting gamers will not be limited to their number, as the online console gamer base alone will reach 165 million by 2017, but also their hardware. Gamers use computers with higher processing capabilities to handle intense game play. Unfortunately, that same processing power can be exploited for Bitcoin mining. We've already seen this happen before; with the rising adoption of the cryptocurrency, it certainly won't be the last.
THE WAIT FOR THE “KILLER APP”

We will see a lot of small technical innovations but no major breakthroughs in cybercrime. Cybercriminals will continue to wait for the “killer app,” that one technological breakthrough that will get mass appeal. While certain smart gadgets have already been made available to the public, none have captured the public's attention in the same fashion as previous breakthroughs like the iPod®.

GOING BEYOND 2014

The “next big thing” that cybercriminals are waiting for could come from the world of augmented reality (AR). Virtual reality headsets will become a disruptive technology. Not only will they change the gaming space, they will also be used for other purposes like attending conference calls and posting on social networks.

These smart devices will become more desirable as the years progress. Expect isolated attacks to start in a couple of years. These AR headsets will become the new favored target to obtain personal information. Their built-in cameras will be used for privacy attacks, giving cybercriminals a bird's eye view of users' daily activities and a means to record details like bank PINs and other personal information.

Drones will be used for surveillance and farming. They will become common and standardized in the commercial space. Unfortunately, cybercriminals can and will exploit them as well.

Beyond 2014, radio-frequency-enabled technologies will become real attack targets. We could see an AIS transmitting station attack by 2020 that will have drastic consequences for the shipping industry.
PROTECT YOUR NETWORK

Organizations should begin at the core. Protecting your core data or “crown jewels” is a priority, as this is a favored threat actor target. They will try to get inside corporate networks to steal data.

Classify the data (e.g., blueprints and databases) in your core. This will help you assess which requires additional protection and identify the steps you should take.

It’s best to assume that someone is already inside your network. Make sure your organization uses the proper tools and protocols to properly protect your network. Proper employee education will also help mitigate risks associated with data breaches.

Adopting consumerization means considering the creation and implementation of a comprehensive set of security guidelines for all kinds of devices. Note that attackers can and will use any device to get in to target networks.

PROTECT YOUR DEVICES

Protecting your digital life means protecting every device you own. The volume of malicious and high-risk Android apps is projected to reach 3 million by 2014, so securing your Android device is a must. Even with the rising popularity of mobile devices, don’t ignore your computers. Install and regularly patch security software to stay safe from attacks, especially those that rely on vulnerability exploitation.

With so many Internet-ready devices, you should also secure your home network. A secure network is the baseline for security, especially for devices that lack security features or options.

PROTECT YOUR PRIVACY

Always remember that cybercriminals want to get their hands on your precious data. Take extra care when accessing your online accounts via any device, especially those that require revealing personal information.

Be mindful of the amount and type of information you share online. Always think twice before posting anything online. Read the fine print before signing up for any service; it may be asking for your information as payment.