THE ULTIMATE HUB FOR SECURITY

Visit Our Microsite To Access:
- Free Assessment Tool
- How-To Content From Our Partners
- The Latest Security News And Updates

>> ACCESS THE MICROSITE NOW <<
Welcome to the Softchoice Ultimate Security Guide

The intent of this guide is not to help you select a vendor product. More importantly, it’s intended to help you navigate through the latest security threats to minimize exposure and risk to your brand.

With approximately 20 years in IT in both hardware and software, I have never witnessed a bigger disruption than today. More organizations than ever are looking to transform their businesses to embrace the opportunity of social, mobile, analytics and cloud tools. However, IT providers offer a plethora of digital tools and services, making it challenging for our clients to balance the pros and cons of a new "digital" business reality.

Also, how do you take advantage of this new digital transformation to help differentiate your business in the market?

Intel has called this the 3rd industrial revolution, or the New IT platform - the convergence of Social, Mobile, Analytics and Cloud. How do you move workloads to the cloud, how do you get to more customers, how do you get the influencers that use different methods to formulate ideas?

What are the implications of moving to the cloud, or taking advantage of hybrid IT? How do you deal with the proliferation of mobile devices - 50 billion to be connected by 2020?

Ultimately, how do you strengthen the brand of your organization? You do it securely.

The goal of our security team is to help you understand that there is no silver bullet solution to help you completely prevent your organization from being compromised.

There is no endpoint, gateway or firewall sophisticated enough to do this alone. There is no individual service that can do this for you either.

Remember, cyber criminals only have to be successful once to wreak havoc - while you need to ensure business continuity all the time!

At Softchoice we strive to be part of your team and to help you uncover and understand the risks that exist, specifically those that prevent you from reaching your ultimate business goals. We do this by working closely with your team to develop a roadmap and process to successfully secure your environment.

That is why we have aligned ourselves with the leading security players in the world to make that happen.

Yours truly,

George Myrtos
Category Lead, Business Development
Softchoice Enterprise Software & Security
Issue 2

Complete List. What’s in This Issue

Confessions of a Hacker

Why 2016 Will Be the Year of Internet Insecurity

Mobile App Mismanagement

Six Rules for Safe Schools: Protecting Educators and Students From Advanced Web Threats

Why Infosec Pros Should Keep a Close Eye on Cyber Efficiency

The Wind That Smells Like Rat: The Story of Adwind MAAS

Simplifying the Vendor Jumble: Why Vendor Consolidation Is More Important Than You Think

A New Platform Brings New Risks: Making the Case for Security Beyond the Network Perimeter
Meet Our Dedicated Security Team

ANDREA KNOBLAUCH
PreSales Technical Architect

ANDREW CAMPBELL
PreSales Technical Architect

CHRIS WALSH
PreSales Technical Architect

GEORGE MYRTOS
Category Lead, Enterprise Software and Security

JEFF KROTH
Security PreSales Architect

JEREMY BANDLEY
PreSales Technical Architect

MIKE COIT
PreSales Security Architect

MIKE STINES
PreSales Security Architect

TREVOR MULVIHILL
PreSales Technical Architect

CONTRIBUTORS

Amanda Brown
Marketing Manager

Chelsey Byng
Marketing Operations Lead

Emily Davidson
Content Marketing Lead

Keith Mclean
Graphic Design

Martin Pietrzak
Content Marketing Supervisor

Michael Smyth
Marketing Database Lead

Mick Warner
Campaign Design Specialist

Rebecca Tesfagiorgis
Marketing Manager

ADVERTISING INQUIRIES

George Myrtos
Category Lead, Enterprise Software and Security
George.Myrtos@softchoice.com

2016 ULTIMATE SECURITY GUIDE

PLATINUM SPONSORS
IBM SYMANTEC

GOLD SPONSORS
DELL INTEL
KASPERSKY SOPHOS
TREND MICRO

SILVER SPONSORS
AVG BLACKBERRY
ESET FORTINET
MALWARE BYTES
You can’t be everywhere. But your security can.

Hybrid cloud security from Trend Micro is everywhere you need it to be. It’s just as smart and dedicated as your staff. Plus, it’s automatic. So if anything goes wrong in your cloud or data center, Trend Micro Deep Security is there to automatically sense it and trigger the necessary actions to keep you protected.

Automate your hybrid cloud security today.

KASPERSKY SECURITY FOR VIRTUALIZATION

• Optimized for virtual servers & desktops
• Solutions for VMware, Citrix & Microsoft
• Helps to maintain high consolidation ratios
• File and network level protection

PLATINUM SPONSORS

GOLD SPONSORS

SILVER SPONSORS

© 2016 Intel Corporation   Intel and the Intel and McAfee logos are trademarks of Intel Corporation or McAfee, Inc. in the US and/or other countries. Other marks and brands may be claimed as the property of others. www.intelsecurity.com.

McAfee is now part of Intel Security.
I am a hacker.
The type of hacker that spends her days uncovering the weaknesses in others. Not just corporate networks, but people as well. At first, I was curious to see how secure companies were when it came to protecting their data, everyone’s data. I wanted to know what made people respond the way they did.

Now, I’m tired of seeing the headlines about large breaches that result in the loss of privacy, and companies that don’t treat sensitive data with the proper (if any) safety controls. Security is merely a “nice to have” and not a critical component driving everything they do. Now, I feel a (slight) internal sense of responsibility to make sure that companies are promoting proper security practices when it comes to managing consumers data.

The first harsh reality is this: for every company that has a solid security plan to help keep hackers like me out, there are another dozen more that demote security to a minimal set of checkboxes and re-allocate funds to other projects.

Not that I am complaining, companies who rely on free endpoint solutions or other minimal security controls to keep me out, just make it easier for me to get in. Those companies just become a larger bullseye for me, simply because I would rather spend less time and go after smaller businesses than try to hack into a large corporation that’s well-invested in a bulletproof security posture.

Risk vs. reward, that is what motivates me, and you would be amazed at the types of data that I can retrieve from many organizations.

I hate to brag, but even companies that are considered impenetrable are no longer immune to my skills. Enter: social engineering and ransomware.

If I choose to send an email to the right people, your average employee, heck even high-level executives won’t be able to resist clicking on links or attachments with super relevant subject lines like ‘invoice’ or ‘past due’. From there I exploit this weakness and inject malware or crypto viruses to encrypt all of the company data. I will force IT teams to either restore from an old backup or pay a ransom - which in many cases will contribute to me accessing their sensitive information.

Whoever was responsible for the Hollywood Hospital ransomware attack made $23,000 in a single day. So, tell me, how often do you back up your critical data?

These types of exploits became many hackers’ go-to methods, as they easily slip past lower-grade security controls, with minimal effort. After all, it’s just an email. You see, no matter how good your security controls are, even if you set up the best firewall or email protection, we will find our way in. It’s just a matter of time and patience, exploiting the right weaknesses.
The minute you move your data to the cloud, or connect anything to the Internet, your data is exposed.

People like me from all around the world are looking for anything they can use to profit, and smaller organizations are a great gateway to get into larger ones. For example, small branch offices with lax security controls that connect to corporate headquarters, unsecured Point of Sale (POS) systems at the local retailer and -my personal favorite- unsecured hotel Wi-Fi. These become entry points for many of us, with a lot less risk than going after larger corporations. But large corporations aren’t safe either; they just require a different set of tools. I can take down your network with a DDoS attack for the price of a fast food combo – which means your entire network including data stores and applications are rendered inaccessible. Personally, I show little regard for the damage that is caused by breaching one of these organizations. I justify it as a cost of business. After all, it wouldn’t have happened if they had better security controls.

The second harsh reality is: hackers like me attack corporations, well, because we can.

We no longer need a reason, we cite corporate greed, or wanting to teach these corporations humility, but in the end, you’re all the same targets to us.

So, why write this letter? I want organizations to stop overlooking security. Hackers aren’t going away, in fact, we are evolving and growing right alongside the latest security controls.

You need to protect your endpoint devices, file servers, confidential information, mobile devices, applications, internet access, corporate mail, web gateways, and collaborative solutions.

How much would you pay to get your customer data back?

Listen, until you start to take security seriously, and build it into every part of your organization, you will always give hackers a reason to do what we do. Want to know how to stop me? Put enough security controls in place to get me to move onto the next guy who doesn’t take security as seriously.

The End.
Why 2016 Will Be the Year of Internet Insecurity

Cyber attackers are developing new methods to dodge, circumvent, and leapfrog defenses in ways that leading internet security companies are unable to fully anticipate. From the ground up, from personal use to enterprise-level security, the breadth and depth of cybersecurity threats grows on a yearly basis — the amount of breaches increased by 23 per cent from 2014 to 2015.

But cyber security analytics experts are reinventing the approach to building cyber defenses, by focusing on vulnerabilities and the exploits linked to them, rather than trying to address each specific form of attack. As more devices are compromised, cyber security experts have more data to work with to determine what the biggest dangers are going forward and you can learn what to avoid doing right now.

We Connect Everything to the Internet

Ironically, the single biggest window of vulnerability for cyberattacks is the widespread adoption of internet-capable devices, commonly known as the Internet of Things. The Internet of Things has brought us internet-accessible televisions, gaming consoles, smart watches that open windows for data burglars.

Some research firms believe that there will be as many as 6.4 billion connected devices in use in 2016, which is a 30 per cent jump from 2015. By 2020, the amount could climb to more than 20 billion connected devices.

We Download Apps Without Thinking

The race towards a more connected world has seen many developers skipping over the basic security fundamentals in the code of their software as they scramble to meet a rapidly-expanding market. But when developers get sloppy, their customers pay the price. In 2015, Symantec discovered that 52 percent of health apps — a hugely popular mainstay on smartphones and wearable devices — did not even have a privacy policy in place. In addition, 20 per cent of these apps sent all sensitive information (logins, passwords, data) back to their source in unencrypted plain text.

Continued on next page.
Achieve a higher level of security.

- Adversary and Threat Intelligence
- Training and Simulation Exercises
- Incident Response Services
- Advanced Threat Protection

Learn more >>
Indiscretions in consumer-level apps have led many experts to claim that smartphones represent the biggest risk category in cybersecurity going forward. The past year saw increasingly creative (and devastating) trends in the use of malware, Trojan viruses, and other traditional forms of cyberattacks.

Unfortunately, the amount of generally uninformed or under-informed users will always outpace the amount of apps and devices without robust security protocols.

WE PAY HACKERS TO GET OUR DATA BACK

The latest reports show that cyberattackers have taken to infiltrating enterprise networks and rigging the security infrastructure to turn the system against its intended users – extorting employees for cash by holding their connected social media accounts or data hostage until they submit to their aggressors.

Another favorite tactic involves planting fake software updates and simply waiting for companies to download them on their own, spreading the malware without any brute-force hacking required. In fact, five out of every six large companies (with more than 2,500 employees) were targeted by spear-phishing attacks alone in 2014 (a 40 percent increase over the previous year). Unfortunately, same fate awaits small and mid sized organizations. No one is safe...

CYBER SECURITY DOESN’T END AT THE FIREWALL ANYMORE

As much as the state of cybersecurity is always in flux, there are some universal best practices to help minimize your vulnerabilities and make sure your organization is in the best position when cyber attackers have it in their sights.

From a business standpoint, effective cyber security is about building up as many effective and non-redundant layers of protection at every point of your network as possible. From network security, to encryption, to authentication, you need to eliminate any weak points of entry.

By pairing with a dedicated managed security service provider, you can extend your IT team without (unrealistically) expecting your existing team to triple their coverage with the exact same level of human power.

TEACH USERS TO PLAY IT SAFE

In addition, mandatory and ongoing education for all of your employees must be established to make sure everyone is on the same page when it comes to accessing and protecting sensitive data on corporate devices. To make sure everyone in your organization really gets it, run practice drills and allow your people to come forward with their concerns and questions; if someone doesn’t know that they’re doing something wrong, they won’t even be aware of the security risk they present.

When it comes to personal use of connected devices, the key is, as always, to use a strong password. If you want a quick breakdown of the sorry state of the average person’s password, look at this list of the most popular passwords of 2015, and realize why it is almost too easy for a cyberattacker to get access to all of your information with little to no real effort. Use strong and unique passwords for each of your devices, and change them quarterly.

When it comes to social networks, be extra vigilant about what you click; Facebook-borne malware is becoming increasingly common, and the average person usually lets down their guard when they see a link from a trusted friend. But your friend’s account can be compromised just as easily as anyone else’s, so always think twice before clicking through.

Finally (and this one is a pain), take the time to read and modify the sharing permissions for any apps you download to your devices. Key factors to watch for are permissions about sharing personal data and allowing remote access; disable both of these if they’re not absolutely needed for your enjoyment of the app.

Get a deeper dive into the security threats we faced in 2015, by reading Symantec’s 2015 Threat Report.
As mobile device usage intensifies, the number of related security threats thrive at a staggering rate – most of which target iOS and Android devices. The reason is simple: in 2015, users downloaded more than 300 billion iOS and Android apps.

Few users are as vigilant on their phone or tablet as they are with their PC or laptop, since almost no malware targeted mobile apps for many years. Until recently, users did not worry about downloading infected software, and in-house app stores check applications for malware and viruses prior to being released to the public. Today, hackers have discovered all kinds of avenues of attack into the mobile universe.

Once accessed, smartphones offer a treasure trove of personal information: social security numbers, bank information, logins and passwords, pictures of user IDs, bank documents, and confidential business information that are ripe for the picking.

It has never been easier to acquire so much data with a single breach.

Few users read a word of the Terms of Service and simply install the app. In some cases, this means they are handing complete control of their phone to an unknown attacker.
Cognitive security is here.
When everything is connected, everything is vulnerable. IBM uses cognitive technology to help protect the critical assets of your business. It senses and helps detect millions of hidden threats from millions of sources, and continuously learns how to defeat them. When your business thinks, you can outthink attacks.
Take flashlight apps, for example. By installing one, users handed over access to contacts and pictures, allowed outsiders to modify system settings and receive data from the Internet. Most apps request more access than they need, of course, because they are designed to acquire consumer information.

But it is not just user apps that are at fault. Too many companies exhibit a casual attitude when creating their own apps. The Ponemon Institute recently released a report entitled, The State of Mobile Application Insecurity. Researchers found that on average, businesses test less than half of the mobile apps they build. Thirty-three percent of companies never test apps to ensure they are secure before deployment.

In a BYOD world, therefore, a multi-level security framework is required to separate personal and enterprise data, distribute enterprise apps, keep them updated (in terms of functionality and security) and provide secure web access. Such a framework should also include analytics.

For businesses, there is a growing mountain of unstructured data in endless numbers of repositories at both the device and enterprise level. With that in mind, every app must go through a process of security testing to identify any and all vulnerabilities. Testers should verify that all application data is encrypted. In addition, robust authentication procedures as well as access controls for enterprise systems must be in place. That way, even if a hacker gains entry into one device, it doesn’t provide a pathway to data beyond that individual’s pay grade. Testing must confirm that everything is secure before any app is distributed.

An enterprise-grade security platform must be able to detect anomalies in network and application traffic patterns in their early stages in order to root out encroachments before they develop into a serious breach.

The platform must have the capacity, performance and speed to isolate individual threats within vast oceans of data, countless logs and databases within the enterprise.

The appearance of the Internet of Everything means that connected devices can now access each other. Without secure policies in place, attackers have the ability to access connected cars, appliances, lighting, video surveillance systems and, in some cases, software-controlled industrial machinery.

There is no question that mobile devices pose an unrelenting risk for concerned organizations. However, the answer is simple: IT teams must take a holistic approach to securing devices, mobile productivity applications and the access and fraud concerns that come along with them. Once a device-level policy is in place, IT needs to underpin it with an additional layer of visibility through security intelligence. Only by addressing all of these areas can a company truly deploy a comprehensive mobile strategy and protect the assets and reputation of the enterprise.

A very fast way to configure devices for enterprise access is to employ a fully integrated cloud platform, like IBM’s MaaS360 solution, that is able to start enrolling devices in just a few clicks.

Learn more >>

BY 2016, THE NUMBER OF SMARTPHONE USERS WORLDWIDE WILL SURPASS TWO BILLION AND THE NUMBER OF MOBILE DOWNLOADS PER YEAR WILL ECLIPSE 268 BILLION.
SIX RULES FOR SAFE SCHOOLS: PROTECTING EDUCATORS AND STUDENTS FROM ADVANCED WEB THREATS.

If you’re an IT professional, and also a parent, you already know that kids are more connected than ever. At school, these connections push educators to rely on the same technology to transform learning experiences from traditional, chalkboard, one-lesson-for-all instruction, to an on-demand format that students can absorb from anywhere - and even customize to their unique learning style.

However, education IT budgets are tighter. Districts’ technology infrastructures are caught in the middle, requiring K-12 IT administrators to literally do more with less.

Access to libraries of digital content provides teachers a wealth of individual lesson plans that effectively support each child’s learning style. Using the internet, students gain access to the information and sources needed to work independently, or in a group, and submit their own work.

Even though relying on the internet for education opens the door to learning, it also opens the door to risk. Students, faculty, administrators, contractors and parents create a user base at the school with mixed demands – increasing the chances a threat will get past the network.

What K-12 IT administrators need is a network and information security solution that is effective, high performing, flexible and easy to manage.

The use of networks to deliver instructional content cuts materials costs and improves the uniform availability of top-tier curricula. But many of these programs — such as those using video content — require unimpeded high-speed connections. When those connections are slowed by extraneous use, some of that value is lost. Increasing bandwidth just shifts the costs and sets the stage for more problems down the road.

Online administrative tools simplify implementation of district-wide programs and policies. They enable anytime, anywhere access to resources and communications for faculty, administrators and students. But the proliferation of mobile endpoints and the management of access levels can quickly present a challenge.

Since so much of this functionality is browser- and internet-based, the traffic can seem like one giant stream. But blocking ports to address threats can seriously impact productive use of the systems.

Wireless access has become a lifeline to faculty members and their students. But wireless connections — intended to allow quick and easy access to the network — are vulnerable to intrusion and, because access points are physically distributed, management can be difficult.

Overlaid on the security concerns of K-12 IT administrators is an extensive regime of regulations. Central to this is the Children’s Internet Protection Act (CIPA), designed to protect minors from inappropriate content.
Whether a child is just entering school, or becoming an independent teenager, parents rely on IT administrators to regulate internet access and the types of content available for students. Even the private sector weighs in here with liability issues regarding the transfer of copyrighted content.

Districts must take all reasonable steps to satisfy these regulations. In fact, they must be able to demonstrate their compliance, which requires management tools that allow for deep visibility into network activity and detailed record-keeping.

However, K–12 districts simply do not have the financial resources to make IT security their first priority. This is not just a matter of buying new equipment or services. Any new equipment also requires deployment.

In order to achieve a high level of security without impacting the user experience, IT teams must make sure traffic is thoroughly scanned with minimal latency.

To meet these requirements, multi-gigabit throughput rates have become standard for Next-Generation Firewalls, or NGFWs.

**WHAT TO LOOK FOR IN A NEXT-GENERATION FIREWALL**

1. **Legacy features**: An NGFW includes all standard capabilities found in a first-generation firewall i.e. packet filtering, stateful packet inspection, network address translation, and high availability.

2. **Integrated IPS**: Effective intrusion prevention systems require advanced capabilities to combat evasion techniques and enable scanning and inspection of inbound and outbound communications to identify malicious or suspicious communications and protocols.

3. **Application intelligence and control**: Application awareness and control includes protocol level enforcement, full-stack visibility with granular application control, and the ability to identify applications regardless of port, or protocol being utilized.
4. **Extra-firewall input:** User-ID awareness enables administrators to enforce application policies based on AD user/group (without having to trace IP address to user ID), adding insight into usage and traffic.

5. **Adaptability:** Another important capability of NGFWs is the dynamic adaptation to changing threats. This means devices must be updated constantly with new signatures to stop threats, and stay on top of the evolving malware landscape.

6. **Payload scanning and performance:** All of the above requirements demand full payload scanning at optimal throughput rates in order to avoid having to sacrifice security for performance.

For effective threat protection, organizations need best-in-class firewall and intrusion prevention - without the complexity of managing separate appliances, GUI’s and deployments.

NGFWs with intrusion prevention capabilities deliver enterprise class resistance to evasion, powerful context and content protection capabilities as well as comprehensive threat protection and application control in a single integrated device.

For example, an NGFW enables utilization of [YouTube for Schools](https://www.youtube.com), offering students structured access to YouTube’s educational content while blocking recreational access and content.

[Learn more about Dell SonicWALL solutions for K-12 here >>](https://www.dell.com)

---

**Helping schools secure their networks**

**Smarter security appliances to protect networks and budgets**

**Learn more >>**
The intense demand for trained information security and privacy practitioners is reflective of the convergence of technology, productivity, and profitability.

CIOs and CISOs that balk at enabling more mobile, cloud, and Internet of Things (IoT) tools not only find themselves in a cultural conflict, but also at odds with the business or mission of their organization.

WHY INFOSEC PROS SHOULD KEEP A CLOSE EYE ON CYBER EFFICIENCY

NO ORGANIZATION WILL EVER BE IMPERVIOUS TO BREACHES, BUT EFFICIENT ORGANIZATIONS CAN LOWER THEIR OVERALL RISK AND SPEND.

By Scott Montgomery,
VP & Chief Technical Strategist, Intel Security

Intel Security’s McAfee Data Exchange Layer eliminates cumbersome and high-maintenance point-to-point product API integrations with a solution that gathers all components in a single cohesive system, regardless of vendor or underlying architecture. Simply integrate your security solutions once into DXL to start publishing and subscribing to information from other products and solutions running on McAfee DXL in your environment. Learn more at mcafee.com/us/solutions/data-exchange-layer.

Make smart security decisions, faster.
For instance, Boston Consulting Group indicated that the remote cardiac monitoring market in the US alone would eclipse $1 billion in 2016, a specific example of the convergence between technology, productivity, and profitability.

The ability for a doctor to remotely adjust a pacemaker without a patient visit or in an emergency situation has a profoundly positive impact on patient care. Information security and privacy professionals simply must find a way to enable this kind of technology while encompassing the risk as best they can.

At the same time, there is a systemic personnel problem. There are simply far too few trained information security and privacy practitioners available to organizations. The baby boomer generation is taking decades of experience with it into retirement; and the prospects for replacing them are bleak.

The 2015 (ISC)2 Global Information Security Workforce Study estimates two global labor gaps:

- The gap between the existing workforce and what the respondents’ companies are funded to hire (600,000 workers).
- The gap between the existing workforce and what those companies believe they need (1 million more workers).

As more devices become IP-enabled for the first time and need to be incorporated into an organization’s information security and privacy posture, the tax upon practitioners will become even more pronounced. Also, for the first time in the (ISC)2 study, practitioners have become acutely aware that the premise that they’ve used for the last 20 years - buy unique tools for each specific IS and privacy problem - has created an unwieldy “sprawl in security technologies.”

All of these conditions - demand, expanding IP footprint, convenience, cost reduction, and insufficient trained practitioners - create an untenable competition between business or mission enablement and security. Evidence of this competition can be seen in the dramatic increase in time from breach detection to remediation. The (ISC)2 study results show a troubling trend indicative of a workforce stretched by demand and sprawl, as indicated in chart above.

It is for these reasons that dramatic improvements in both efficiency and efficacy should be the goal of any decision IS teams are considering.

Any decision regarding methodology, vendor, product, or service that doesn’t demonstrably increase efficiency and efficacy is a bad decision.

Organizations that invest in streamlining their infrastructure to become more streamlined, automated, interoperable, resilient, sprawl-reducing,
and focused will stay ahead of the math and enjoy the most important results.

No organization will wind up impervious to breaches, but efficient organizations will lower their overall spend by:

- Consolidating the number of vendors, tools, and services they use
- Reducing their labor-hour costs by ensuring automated means of execution
- Reducing the number of events that operators and analysts need to respond to manually
- Shrinking the hours operators and analysts spend by reducing events requiring follow-up to fewer, more noteworthy events

The time between breach and detection and the time between detection and remediation will drop measurably, ensuring that breaches don’t have a material effect on the business or mission of an organization.

At last October’s FOCUS’15 conference, Intel Security leaders previewed a new standard in which the Threat Defense Lifecycle will provide you with the right tools needed in the face of this impending threat landscape.

This portfolio will continue to focus on industry leading solutions to protect against known threats and breaches, but also shift greater attention to provide and integrate tools to detect threats faster, and enable automated workflows to more quickly correct them - an integration between a dynamic endpoint solution, intelligent analytics, cloud-delivered security, and centralized management.

Learn more >>
The idea of renting out malware is not new. Successful malware writers soon hit on the idea that offering their creations to ‘people-with-a-purpose’ could be much more profitable than scouring the Internet themselves in the hope of a big catch.

Yet offering a service proved even more profitable. It delivers convenience and simplicity to a much broader clientele, who might otherwise be incapable of using malware themselves (and lack the funds to hire mercenaries ready to do their bidding). Such a wide customer base could be expected to ensure a strong and steady income stream.

The creator of the Adwind Remote Administration Tool felt he could have it all, and more, if he could broaden, not just the customer base, but also the range of affected platforms. So how did that work in practice? Let’s see.

A RAT WITH MANY NAMES AND FACES

At the end of 2015, an attack on a particular bank in Singapore was attempted. When the attack was discovered, a peculiar specimen of malware came under the microscope of the Kaspersky Lab Global Research and Analysis Team. It was written entirely in Java, and so could be launched under Windows, MacOS, Linux and Android alike. It also possessed surprisingly rich functionality – and considerable resilience to existing security solutions’ detection methods.

Such a unique combination of features captured the full attention of Kaspersky Lab’s experts – which in turn led to some interesting results. The malware turned out to be one with many names – including Adwind RAT, Frutas, AlienSpy, Unrecom, Sockrat, JSocket etc. – and a short but spectacular history.

It was conceived between 2011 and 2012 by a member of a certain Spanish-speaking hacking forum. The first public release of the Frutas (as it was called back then) malware was in January 2012.

The author worked away steadily, and soon its resistance to detection and broad functionality earned the malware wide popularity in the cybercriminal world. Since then, it has changed hands and names several times, gaining in popularity and being continuously improved.

Little more than a year after its debut, a subscription model was offered, turning Adwind into a full-scale example of easy-to-use MaaS (Malware-as-a-Service). At the same time, the malware began appearing in targeted attacks across the globe.

The most recent incarnation of this peculiar malware goes under the name of JSocket. It is hard to credit, but its proprietors openly advertise it, as though offering something quite legitimate; and their shadowy hosting provider has so far avoided being located.

Hard to believe these slick, user-friendly webpages are offering highly criminal services.

Would-be customers register with a valid email address, choose a subscription plan – and are even ‘upsold’ a wide choice of optional additional modules.
A PURPOSEFUL AND TALENTED RAT

A phishing email with an attachment is the most common starting point for an Adwind-based targeted attack – that or just ‘sand washing’ in search of something useful. The attachment usually looks like a .JAR file, obfuscated and packed several times to complicate detection by static mechanisms. Sometimes it is embedded within an .HTA or even a .DOC/.RTF file. To further confuse existing Windows security systems, the authors purposely use case-sensitive filenames and some other artifacts of *NIX-based development.

Once the attachment is clicked on, the main backdoor is executed. Aside from being able to download and run additional tools, it possesses very broad functionality in itself. For example, it enables the operator to obtain extensive system information, steal passwords, clipboard contents and cryptocurrency keys, record video and audio, grab the keyboard input or set up a proxy server. The attacker can even start a chat with the victim – though it’s difficult to imagine quite how this would go.

The number of known C&Cs is quite extensive and encompasses many geographic regions. There is proof that some Adwind-based targeted attacks directed at Asian-Pacific companies, with major focus on financial institutions, can be linked to the criminal activities of Nigerian immigrants in Malaysia.

Meanwhile the most attacked regions, regardless of motive, are now Russia, the UAE, Germany, Turkey and the US.

HOW TO TRAP THE RAT

Due to the specifics of pure-JAVA malware, as well as massive packing and obfuscation, many anti-malware engines have problems with Adwind detection. But with extensive Security Intelligence at their disposal, combined with leading-edge detection algorithms powered by continuously running in-Lab Machine Learning processes, Kaspersky Lab’s products are able to detect Adwind samples.

Given that (spear) phishing is the main attack vector, setting up a reliable mail security system is extremely important. Kaspersky Security for Mail Servers (which includes a version for Linux) comprises multiple mechanisms to detect and block these dangerous emails. Together with both signature and non-signature malware detection, the solution includes Anti-Phishing supported both by heuristics and by a cloud-assisted reputation system. These technologies allow the detection not just of mail attachments, but also of emails themselves (especially important given that Adwind operators are often careless about their phishing, and casually re-use them).

A JAVA machine can be a very vulnerable system component nowadays, and, especially in businesses like the banking, workstations performing only a limited number of tasks should ideally be stripped of it completely if mandatory software does not require it. If there is need for it, we recommend restricting some of the double-edged functionality, which could cause considerable harm if abused.

Kaspersky Endpoint Protection for Business comprises a Host-Based Intrusion Prevention System (HIPS, also called Application Privilege Control) providing the administrator with four restriction categories depending on trust level; these groups are also shared with an Application Firewall. To reduce risk, the JAVA interpreter can be put into the Highly Restricted group, severely limiting its (potentially dangerous) capabilities. And if you need to disable JAVA selectively with considerable ease, you can do it by setting up a custom software category and restrict its use on selected endpoints.

It also worth noting that Adwind’s mass phishing emails are often rather unsophisticated, relying on employees’ carelessness and inattentiveness; how many employees would normally receive .JAR files anyway? Such
phishing mails being acted on may suggest a lack of understanding of basic cybersecurity principles. This can readily be improved with the help of Cybersecurity Awareness Training available from Kaspersky Lab.

All in all, using multi-layered security is crucial today – as many reports including the widely known ASD Mitigation Strategies keep emphasizing. And it is obviously simpler and more convenient when the majority of these layers are provided by a single vendor and managed through one unified administration console.

Don’t underestimate the risk: any schoolboy today with a bad attitude and $25 in his pocket could potentially arm himself with an extremely powerful and dangerous toolset offered by Adwind, and do a great deal of harm – even to an Enterprise of considerable size. Highly motivated cybercriminals can do much, much more. Clearly, it is time to arm yourself with a proper RAT-catcher – from the leader in the IT Security Industry.

Kaspersky Lab’s products detect different variations of Adwind with the following verdict:

HEUR:Backdoor.Java.Generic

To know more about Adwind, read this blogpost on Securelist!

¹The administrator should test the policy carefully before implementation, to ensure any necessary JAVA-based apps functionality is retained.

KASPERSKY SECURITY FOR VIRTUALIZATION

Protect Servers, Desktops & Data Centers
- Optimized for virtual servers & desktops
- Solutions for VMware, Citrix & Microsoft
- Helps to maintain high consolidation ratios
- File and network level protection

Learn more >>
IT Complexity has never been more acute. Factors such as the cloud, mobility, virtualization, the Software Defined Data Center (SDDC), the Internet of Things (IoT) and Big Data are driving a new period of technology and business transformation. As a result, whole new business models are evolving. Who would have thought that one of the world’s biggest retailers (Alibaba) would have no inventory or the largest taxi service (Uber) would have no cars?

Technology is opening the door to new ways of doing business that adds convenience, efficiency and reduced cost.

But there is a dark side to this transformative period. As companies rush to deploy the latest and greatest tools, they end up with a plethora of technologies and systems that integrate poorly, if at all.

The resulting IT infrastructure would make a Rube Goldberg invention look simple in comparison. IT staff waste half their time jumping between multiple interfaces, writing scripts to move data from one system to another and troubleshooting endless compatibility issues.

While this may be viewed as merely inconvenient from an operational standpoint, it is a disaster waiting to happen on the security side. Companies, these days, typically have an endless catalog of point solutions to address every possible security category. They have several tools to deal with network security, firewalls, intrusion detection systems and intrusion prevention systems. They have another bag of tricks to deal with antivirus (AV), malware, ad blocking and spam. They have liberal sprinkling of endpoint security suites, encryption, public key infrastructure (PKI) products and analytics engines.

Those left with the job of overseeing an organization’s security face a Herculean task of sifting through thousands of event logs and alerts to isolate actual threats. Once they find something suspicious, they have to hop across half a dozen or more screens to determine if there is an actual threat.

This might have been workable ten years ago, but in the threat landscape of 2016, it is a recipe for data breach headlines.
After all, the speed with which the bad guys can infiltrate, compromise information and disappear, is such that rapid detection and remedial action is a must.

This new world of threats calls for a change of the approach. The days of best-of-breed point products are now coming to an end as the liabilities of this haphazard security frontier are continually being exposed to the glare of adverse publicity and an erosion of customer trust.

**A NEW ERA OF SECURITY CONSOLIDATION**

We are entering a new era of consolidation as the solution to ongoing security chaos. Selecting one security vendor capable of effectively handling all zones of information protection leads to benefits such as:

- A rapid ROI from cost/time savings
- The elimination of security complexity
- The ability to respond to, and neutralize threats in real time before serious damage takes place

**ON THE FINANCIAL FRONT, THOSE ORGANIZATIONS THAT HAVE TRANSITIONED TO HAVING ONLY ONE TRusted SECURITY PARTNER HAVE REALIZED MAJOR SAVINGS...**

By no longer having to install, operate, integrate and manage multiple disparate security systems. Having one comprehensive and fully integrated security suite that reaches from one end of the enterprise to the other, means fewer employee hours spent on fewer tasks, freeing up time for IT to invest in strategic projects.

The ROI from this transformation is rapid and manifests in many ways: Speedier time to launch, increased buying power, economies of scale by dealing with one source, simplified personnel training on security systems and an end to vendor finger pointing-are a few of the advantages.

When security specialists are no longer bogged down by the complexity, and tedium of managing multiple tools, they have the time and ability to get a holistic view of the entire enterprise threat landscape.

Continued on next page.
This enables them to isolate potential threats long before they breach the defenses and take action to keep the enterprise secure in an ever more dangerous environment. The value to the organization of this transition in security perspective is immense. Consider that the Verizon 2015 Data Breach Investigations Report found that 80,000 security incidents were reported in one year out of only 70 large organizations surveyed. While IT dealt with the bulk of these encroachments, more than 2,000 serious security breaches occurred.

This is particularly disturbing in view of the fact that these companies were already heavily invested in the latest security technologies.

The cost of each serious breach reached into the millions of dollars in some cases either from theft, damage to corporate image, bad press, customer churn and stock price drops.

At the end of the day, it’s up to the IT team to design a holistic security stance that’s well prepared for modern threats. To decide if a consolidated strategy is for you, you must gauge your risk by discovering how many point products you actually use, and the cost of the IT team’s time maintaining them. Then, add the cost of downtime and decide – is it worth the risk?

To dive deeper into the benefits of security consolidation, view Sophos’ Synchronized Security: A Revolution in Protection.

SECURITY CONSOLIDATION ASSESSMENT

Through our four step approach, we help maximize your security investments, saving you 40 to 60% on your security spend while improving your overall security posture. Simplifying management and reducing cost is well within reach.

Learn more >>
A NEW PLATFORM BRINGS NEW RISKS:
MAKING THE CASE FOR SECURITY BEYOND THE NETWORK PERIMETER

Considered the “third platform” by IDC, dynamic datacenters are answering the call to support gargantuan user demands for applications that support social, mobile, analytics and the cloud.

Examples of these infrastructures include Hilton Hotels, the Office of Personnel Management and Ashley Madison – all of which have suffered high-profile data breaches.

For the modern business, a platform that is scalable, reliable and fast is a must. However, to keep out the modern hacker, protection must extend deep into the network perimeter.

With such high profile hacks, companies are taking notice, and investing. IDC predicts that 40% of security revenues will become tied to predictive capabilities, and protecting the mobile cloud will account for 35% of enterprise security products sold.

As companies take advantage of the operational and economic benefits of virtualization and the cloud, it’s critical to secure their virtualized data centers, cloud deployments, and hybrid environments effectively.

Any neglect to one aspect of security, and you leave gaps that open the door to web threats and the serious (and very public) data breaches mentioned above. Furthermore, to meet data privacy and compliance

You can’t be everywhere. But your security can.

Hybrid cloud security from Trend Micro is everywhere you need it to be. It’s just as smart and dedicated as your staff. Plus, it’s automatic. So if anything goes wrong in your cloud or data center, Trend Micro Deep Security is there to automatically sense it and trigger the necessary actions to keep you protected.

Automate your hybrid cloud security today >>
regulations, you may have to demonstrate that you have the appropriate security, regardless of your computing environment.

Whether you are operating in the data center, or the cloud—you must be able to manage a broad set of security capabilities across multiple environments, ideally from a single platform.

When shopping for a provider, look for a company that leads with the value of server security for physical, virtual, and cloud environments. Instead of managing many point solutions, you can shop from a single vendor to get a complete set of security capabilities with automated management that dramatically reduce both risk and cost.

First, decide what you need to protect. If you’re protecting a data center, you want to consider a solution optimized for VMware virtual environments, including the latest developments such as NSX, as well as virtual desktop infrastructure (VDI).

A virtualization-aware security solution is critical to address the risks posed by the third platform.

For the modern datacenter, a security platform that extends deep beyond the network perimeter will shield unpatched vulnerabilities from attack when hackers get past the perimeter, and stop them at the server. It reduces exposure to these attacks using a host firewall - Blocking attacks and limiting communication to only the ports and protocols necessary (with the ability to log and audit traffic for compliance reporting at the instance level).

To protect the cloud, application and data security needs must be met, while maintaining compliance.

This translates to ensuring server security for cloud instances while simultaneously managing security on virtual and physical servers in the data center. When choosing a solution, you want something simple, with a workload aware policy, and effective administration and reporting tools to give you an up-to-date view of the entire environment.

The desired security architecture is illustrated in this graphic by Trend Micro:

A solution with a workload-aware policy and integrated administrative console will give you a single, up-to-date view of the security posture for your entire cloud environment, reducing time and resource costs by making security management more efficient. Automated vulnerability shielding prevents the disruption of emergency patching.

Lastly, you should look for a solution that integrates with:

- CS P platforms and developer tools like AWS, Microsoft Azure, and VMware vCloud Air
- Cloud deployment tools like Chef, Puppet, RightScale, OpsWorks, Salt, etc.

At the end of the day, you (or your IT team) must provide the most complete set of security capabilities available, like Trend Micro’s Cloud and Data Center Security solution for security beyond the network perimeter, to stop attackers even if they breach your firewall.
HOW WELL DO YOU KNOW YOUR SECURITY ENVIRONMENT?

We designed this free, interactive assessment for you to find out - and get immediate results.

Take your Security Assessment HERE >>