wontok™ SafeCentral SafeDesktop

Financial Institutions: How to Protect Customers from Advanced Malware in 2016

Executive Summary

Modern malware can empty bank accounts in seconds.

Through 2016, this widespread threat will continue to grow unabated. This paper discusses two of the primary mitigation vectors that can be used against such powerful financial malware - backend protection and specialized endpoint protection - and how to identify which is best suited for your environment.

Malicious software (aka malware) affects us all. Modern malware ranges from keyloggers, to ransom ware to spyware to botnets. Arguably the most advanced are financial trojans, which are capable of emptying bank accounts in seconds. The Zeus toolkit has stolen hundreds of millions of dollars globally in recent years, and is one of the most effective financial trojan platforms. This platform has been used to launch other powerful financial malware such as KINS and Citadel, which has stolen millions of dollars from banks in 2015 alone.

The two main mitigation vectors against this blitz of advanced malware are ***backend protection*** and ***specialized endpoint protection***.

Backend protection involves the bank implementing multiple controls which are unseen by the average bank customer. They may involve building out powerful antifraud risk engines built on big data, and implementing dual custody for wire and ACH transactions, and limiting customer transfer limits. They are generally very slow rollouts and resource intensive. As a result, more banks are choosing an endpoint protection solution.

Endpoint protection involves placing software on the customer endpoint, typically PC and Mac devices. Effective end point protection against financial malware is not commonly found in common antivirus suites. Modern financial malware uses techniques such as packing and polymorphic encryption to completely bypass detection by well-known antivirus suites. Zeus has historically been so effective at avoiding antivirus detection that other cybercriminals have adopted its use: Zeus has been used to send spam and steal Facebook credentials in addition to stealing bank credentials since its source code leaked in 2011. **The antivirus detection rate for Zeus on average is still only 40.04%**[1], with many of those detected being early Zeus versions.

[1]*Source: https://zeustracker.abuse.ch/?country=US*

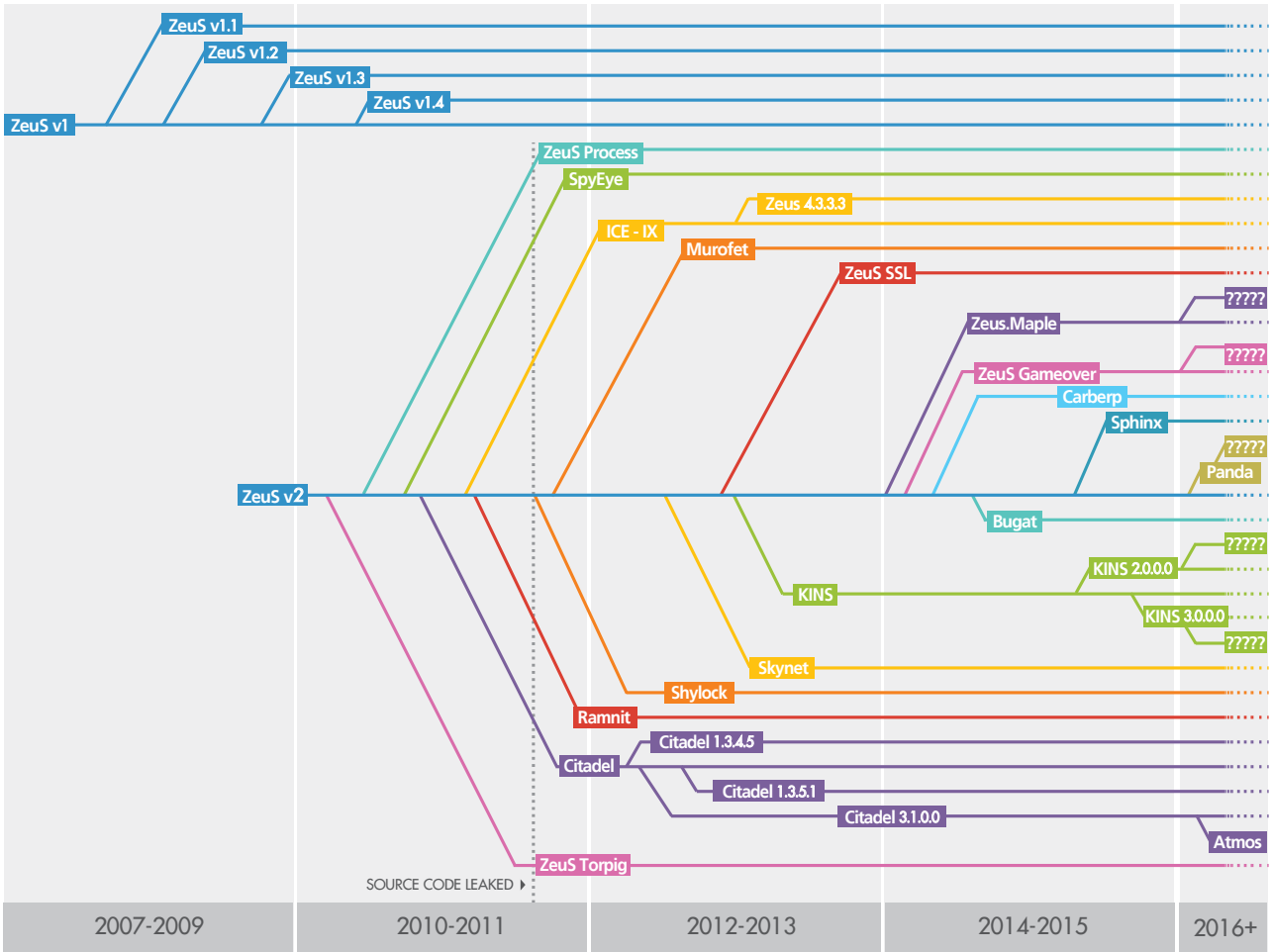
As a result, specialized antifraud tools evolved to combat these threats. Two key types of solution emerged: the minifilter/Browser Plugin and the Secure by Design method. Both have their benefits, but the Secure by Design client benefits are superior and longer lasting than the rapid roll out of the Browser Plugin approach.

Zeus Capabilities

Zeus has powerful keylogging abilities.

Anything typed on a Zeus-infected device is keylogged capturing sensitive data as typed by default and is regularly uploaded to a Command & Control (C2) server. High-risk bank accounts, such as commercial accounts, generally use multifactor authentication for better protection, but even multifactor authentication is compromised by the MitB features of Zeus. Webinjects are highly customizable JavaScript pop-ups purporting to be two-way communications with the bank, taking the form of a request for additional authentication of a customer's identity. Zeus automatically copies digital certificates and can readily overcome this method of authentication.

The Zeus Timeline (2007-2016)



For an overview of Zeus history, read "The Evolution of Financial Malware 2007 - 2016".

Citadel

Citadel is a recent incarnation of Zeus, first appearing in February 2012. The owners of Citadel are actively building on to the source code of leaked Zeus (2.0.8.9), and adding new functionality.

2015 has been a banner year for cybercriminals. Their tools have greatly evolved, and new advanced malware suites are available. Hesperbot, Shylock, Beta Bot, KINS and Carberp are now being used against banks, and this trend shows no sign of abatement. Citadel's successor, Atmos, emerged in the first half of 2016.

Impact of US Court Rulings

When it comes to unauthorized loss of funds from bank accounts, the rules for commercial accounts and personal accounts are quite different.

These rules (Reg E and UCC 4A) form the framework for rights and obligations in litigation.

According to Federal Reserve Board Regulation E (Reg E), if a consumer reports to the financial institution that their card is missing before any transactions takes place, they are not held responsible for any transaction that takes place after the report of a missing/stolen card.

Article 4A of the Universal Commercial Code (UCC) governs the rights, duties and liabilities of banks and their commercial customers with respect to electronic funds transfers. Article 4A was developed to address wholesale wire transfers and commercial ACH transfers, generally between businesses and their financial institutions.

Recent litigation (*Experi-Metal Inc v Comerica, Patco v Ocean Bank*) has clarified bank liability for malware losses on commercial accounts. ***Overwhelmingly where banks have not implemented commercially reasonable security practices and procedures, they have been found liable.*** The elucidation of what is commercially reasonable security has been the subject of litigation.

The courts conclude that banks should be antifraud experts and implement controls, which will greatly mitigate the likelihood of commercial account fraud loss. The courts however, are not expecting banks to provide perfect security to defend against all types of commercial fraud. Rather, the courts take into account the resources of the bank, what peer banks are doing, FFIEC 'authentication in online banking' guidance, and the expectations set by contracts and client interactions. The courts then make decisions based on the evidence collected. As many banks rush to implement effective endpoint protection, those choosing to postpone will likely incur the wrath of the court.

According to experts, based on this trend, other common law jurisdictions (e.g. UK, Australia and India) are likely to follow a similar trajectory.

OVERWHELMINGLY WHERE BANKS HAVE NOT IMPLEMENTED COMMERCIALLY REASONABLE SECURITY PRACTICES AND PROCEDURES, THEY HAVE BEEN FOUND LIABLE.

Ineffectiveness of Traditional Antivirus Suites against Financial Malware

As stated, most common desktop antivirus suites are incapable of detecting and protecting endpoints from modern financial malware.

New financial malware is highly targeted and antivirus vendors do not see copies in the wild until the malware has mainstreamed, by which time cybercriminals will have moved to newer malware having successfully raided countless bank accounts.

TARGETED SCENARIOS

Often, new financial malware is focused on one bank in one country. For example, much of the malware seen in Korean banks is specific to Korea (such as KR Banker) and highly targeted. It is unlikely an antivirus vendor will detect new Korean malware (which may be .00001%) of all new malware. It is even less likely they will build a solution for it, as it affects a tiny percentage of their customers. Then this new update would have to be pushed out to all customers (which can be quick or painfully slow depending on the vendor). It is much more sensible for national banks to invest in a Secure by Design product, which will defeat the malware without requiring any outside help or delay.

Designing a Solution that Works

The pace of financial malware innovation shows no sign of slowing.

As the evidence shows, cybercriminals are still ahead of most banks. And they don't just target large banks. Community and smaller banks can be put out of business within a day by a concentrated attack by a Zeus crew. When designing a solution to mitigate malware on customer machines, there are two principal options: Browser Plugin approach or a Secure by Design approach.

Solution Design 1: Minifilter/Browser Plugin Approach

The lightweight minifilter/Browser Plugin approach at first seems like a great solution. A piece of software is installed as a browser plugin. When the customer visits the bank website, the plugin monitors for 'suspicious behavior' such as webinjects or automated scripting or creating a suspicious VNC connection.

There are numerous problems with this approach:

TIME: In order to validate what is normal vs. suspicious activity, the vendor may have to spend several weeks partnering with the bank, and mapping out their website in detail, learning acceptable values for every single form and every possible response from the bank. Whenever the bank needs to update their website, the vendor must be alerted in advance.

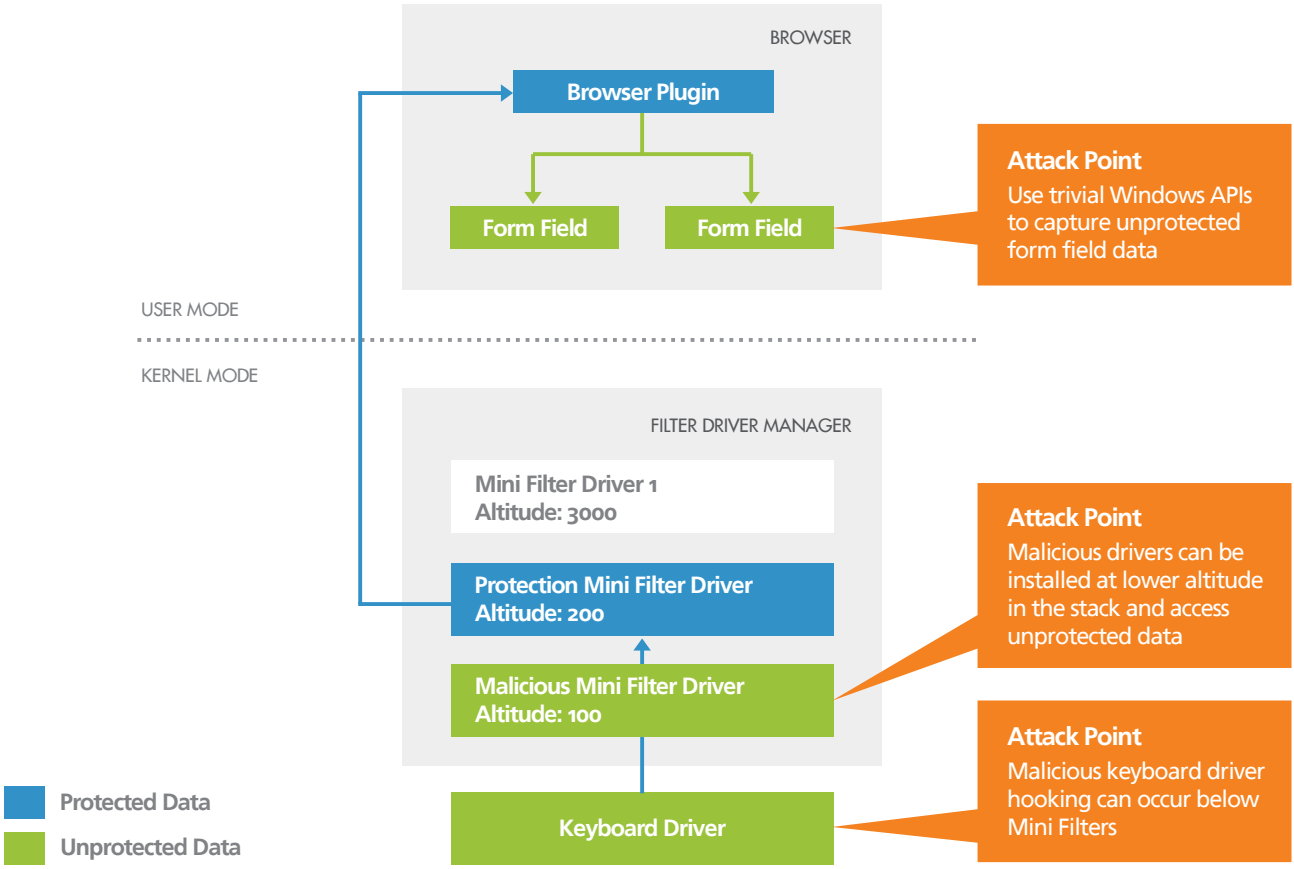
COST: Malware constantly evolves. The vendor must keep a large expensive antimalware team to analyze every variant of malware (perhaps thousands per day) and ensure the product detects these. The product must constantly be updated, causing possible blue screening and incompatibilities with customer endpoints. The costs of such expensive operations are passed onto banks by the vendors.

PRIVACY: In order to collect malware, vendors quite often monitor every web page surfed by bank customers beyond the bank's site, and may have the ability to study how the machine reacts. This creates a huge privacy concern for bank customers.

LIMITED PROTECTION: The solution only protects users when they visit their primary bank, or those of the banks competitors (if they use the same vendor). They are unprotected as they surf 99.999% of the Internet.

Limitations of Solution Design 1: Minifilter Approach

Conventional approach is easily circumvented



Exposed OS Architecture: *Limitations of the minifilter/browser plugin model*

Solution Design 2: Secure by Design Approach

If the antimalware solution was designed to be secure from the very start, by building an malware impenetrable shield around the customer experience, it would have the following effects:

ADJUSTMENT: Customers adjust to a specialized desktop. Most adapt with 3-5 sessions.

Yet this would rapidly overcome and reap the following benefits:

BANK LOYALTY: a) Customers feel secure in the new desktop. This increases loyalty to the bank.

b) The secure desktop can protect customers as they surf the whole Internet. This builds very strong loyalty to the bank.

c) Banks can co-brand the desktop.

LOW CUSTOMER IMPACT: The software is updated on a much less frequent basis.

INCREASED PRIVACY: There is no spying on the customer.

LOW COST: a) No large antimalware team required.

b) No impact on bank website operations.

c) Much lower support costs for the bank.

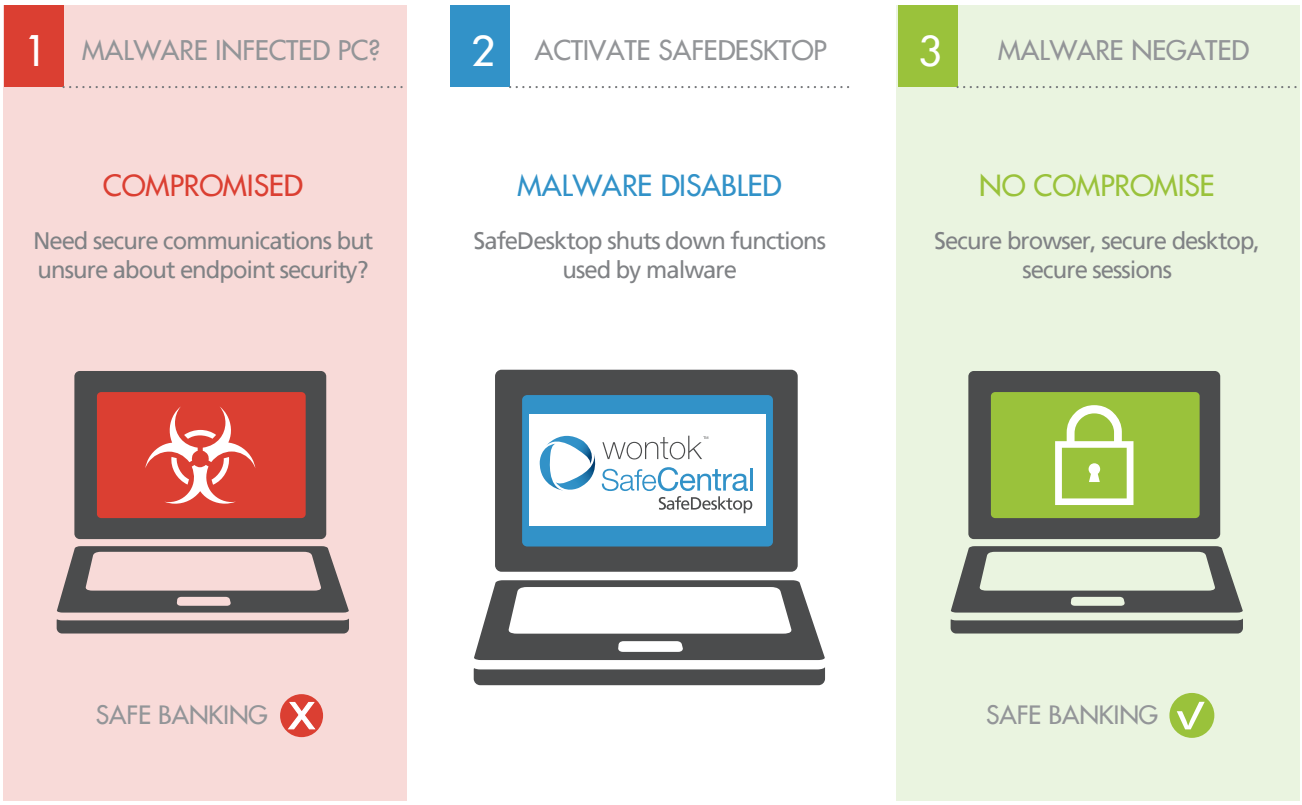
SafeCentral SafeDesktop: Secure by Design

Wontok, the maker of SafeCentral SafeDesktop, is an advanced endpoint security company with a global presence.

Wontok SafeCentral SafeDesktop provides a hardened desktop and browser for Windows PCs and Macs, which is secure by design. Wontok takes the approach that all customer endpoints are already infected and that common antivirus is not effective for the detection and removal of malware. Wontok knows that the best way to prevent cyber theft is to add additional layers of effective protection to existing endpoint anti-malware solutions. The most cost-effective method of defeating ATO malware is the deployment of a competent endpoint solution that is impervious to advanced malware. Wontok creates software that "just works" without having to update itself with every new iteration of malware. This low-cost approach allows banks to significantly mitigate their customers' ATO risk.

SafeDesktop is a one-time-install lightweight software that creates a safe browser and desktop customer experience. It protects sensitive data in use and transactions from being exposed, harvested or stolen. SafeDesktop is easy to deploy and manage. Capable of supporting both Android and Windows devices, it provides a secure desktop complete with a hardened browser where users can initiate protected sessions with their banks or enterprises.

WONTOK SAFECENTRAL SAFEDESKTOP PROTECTS SENSITIVE DATA IN USE AND TRANSACTIONS FROM BEING EXPOSED, HARVESTED OR STOLEN



Even malware-infested machines can be protected by SafeDesktop, minimizing customer impact and costly support calls for banks.

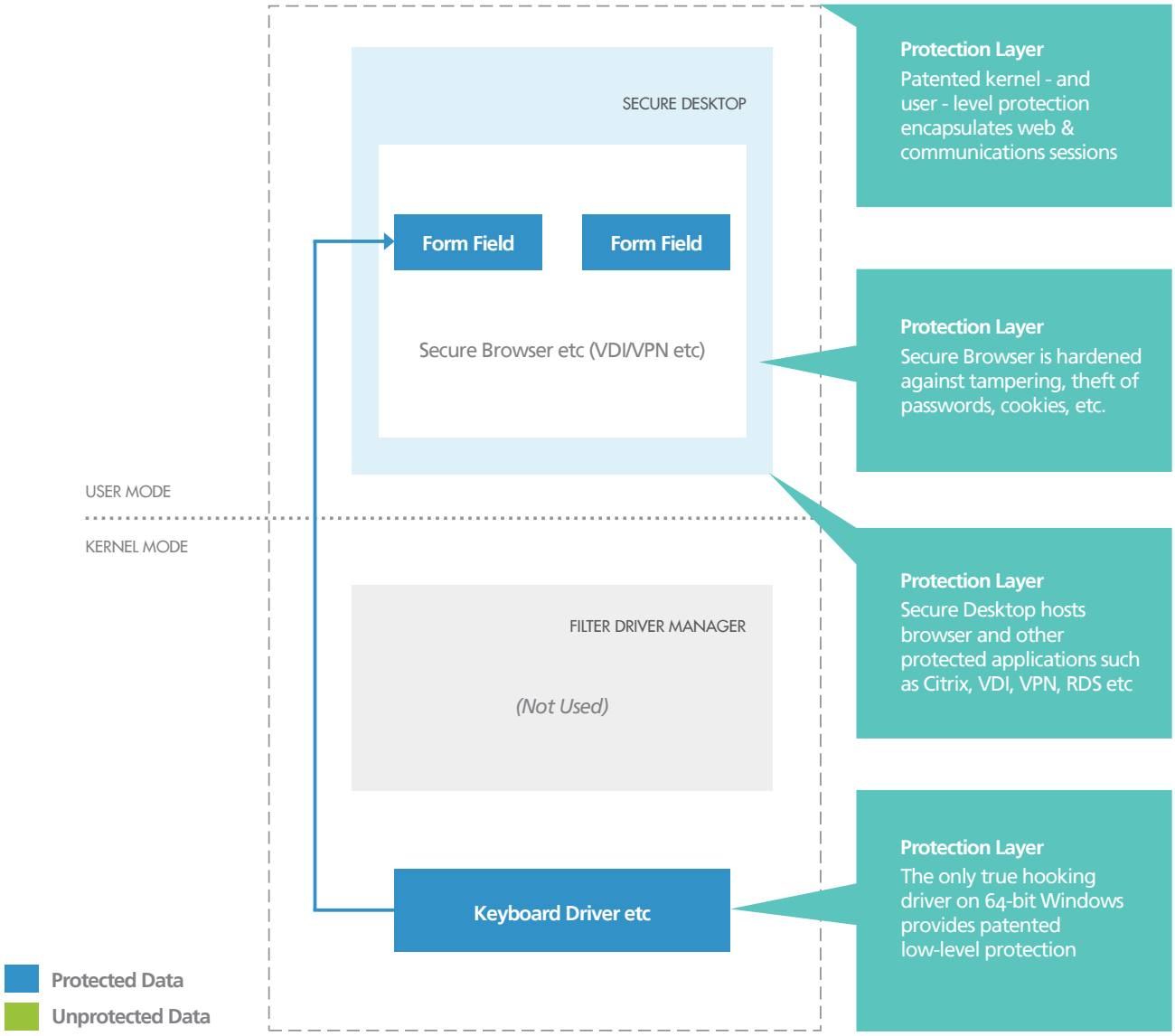
Once installed, users automatically initiate all sessions with their banks using SafeDesktop. Banks can detect whether their sessions are SafeDesktop secured, and they can reject non-secured sessions. SafeDesktop protects entire remote access sessions, from authentication to log out; usernames and passwords are kept safe, secure and barricaded from any malware Wontok has had a high user adoption rate, compared to browser plugin architectures.

A key to SafeDesktop's security is its kernel-level Trusted Security Extension (TSX) technology that locks down the operating system and blocks malware execution on the endpoint. TSX intercepts and interprets over 5,000 discrete Windows commands to block potentially dangerous activities during secure sessions. The product defends against ATO malware, keyloggers, screen capture, phishing attacks, DNS redirection, unpatched vulnerabilities, and registry tampering. SafeCentral also shuts off communications with unapproved domains during secure sessions, thus nullifying ATO malware attempts to communicate with command and control servers and botmasters, which is critical for financial theft. The SafeDesktop browser can be co-branded and can also be deployed in either whitelist or blacklist mode.

TSX INTERCEPTS AND INTERPRETS OVER 5,000 DISCRETE WINDOWS COMMANDS TO BLOCK POTENTIALLY DANGEROUS ACTIVITIES DURING SECURE SESSIONS.

Benefits of Solution Design 2: True Hooking Driver Approach

Used by SafeCentral SafeDesktop and Patented TSX



Secure OS Architecture: *Benefits of the Secure by Design model: Malware simply does not work*

Banks are selecting Wontok SafeCentral SafeDesktop for its effectiveness against modern financial malware, low overhead, ease of deployment and high customer satisfaction ratings. As it is secure by design it will protect your users from the advanced malware of 2016 and beyond.

About Wontok

Founded in 2005 and headquartered in Sydney, Wontok has operations in Australia, Asia and the United States. Wontok has a team of security industry veterans with a proven history of bringing to market value-added security services that fill the gaps left in traditional security solutions. Wontok crafts scalable services delivery platforms and security solutions to be robust and easily deployable to keep up with the demands of business continuity. With ever shrinking margins, Wontok ensures ARPU is maintained through continually evolving value-added services.

Wontok is partner-focused and supports branded or white-label delivery of its world-class security solutions and its value-added services delivery platform. Whether you are a communications service provider, systems integrator, value added distributors, resellers, portal owners, financial institutions or enterprise; visit www.wontok.com for more information today.

Contact Information

San Francisco – USA
americas@wontok.com
+ 1 561 472 5200

Hong Kong
apac@wontok.com
+ 852 2824 8330

Sydney – Australia
anz@wontok.com
+ 61 2 8355 5270

LEDT0021

http://linkd.in/1hZrjk1 Twitter: @SafeCentral

www.wontok.com

wontok™