BLACK COMPUTER

A Technology Primer about ST Engineering Electronics' Trusted Workspace

ST Electronics (Info-Security) Pte. Ltd.
100 Jurong East Street 21, Singapore 609602
T: (65) 6568 7118 F: (65) 6568 7226
(Regn. No.: 199902746G)

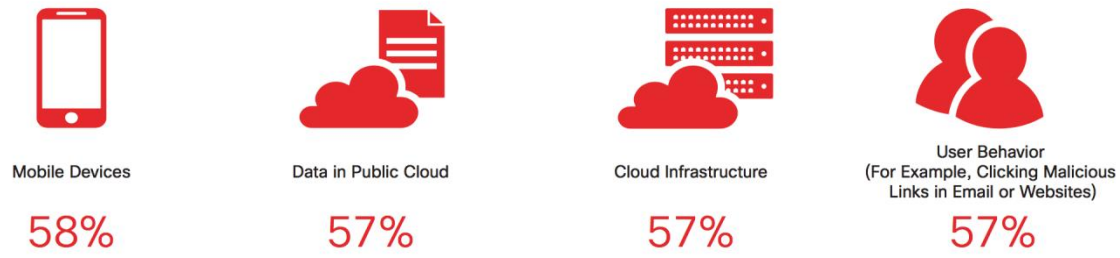
EXECUTIVE SUMMARY

Security has never been so important than before. . It could partly be due to the fact that computing power is becoming cheaper and more new technologies are enabling fast and easy access to tools that were once hard to find. This is particularly true when we talk about computer and network security. At ST Engineering we place great focus on cybersecurity, and our unique solution portfolio enables us to offer both hardware and software-based security solutions to our customers. This document introduces some of the innovative technologies we have in store to help you protect your computer resources.

This document also introduces the current landscape of threats (as of this writing) and elaborates explicitly why the Black Computer solution is needed more than ever.

THREAT LANDSCAPE

We are living in a very interesting time where adversaries have easy access to a vast trove of sophisticated tools and they are not shy of using them. Tools ranging from simple disruption of services to remote organizational resource access and in some cases, hostile takeover for ransom. All these make anyone a little paranoid to say the least. The threat landscape has evolved over the years and the following diagram depicts the evolution.



(Source: Cisco 2017 Security Capabilities Benchmark Study)

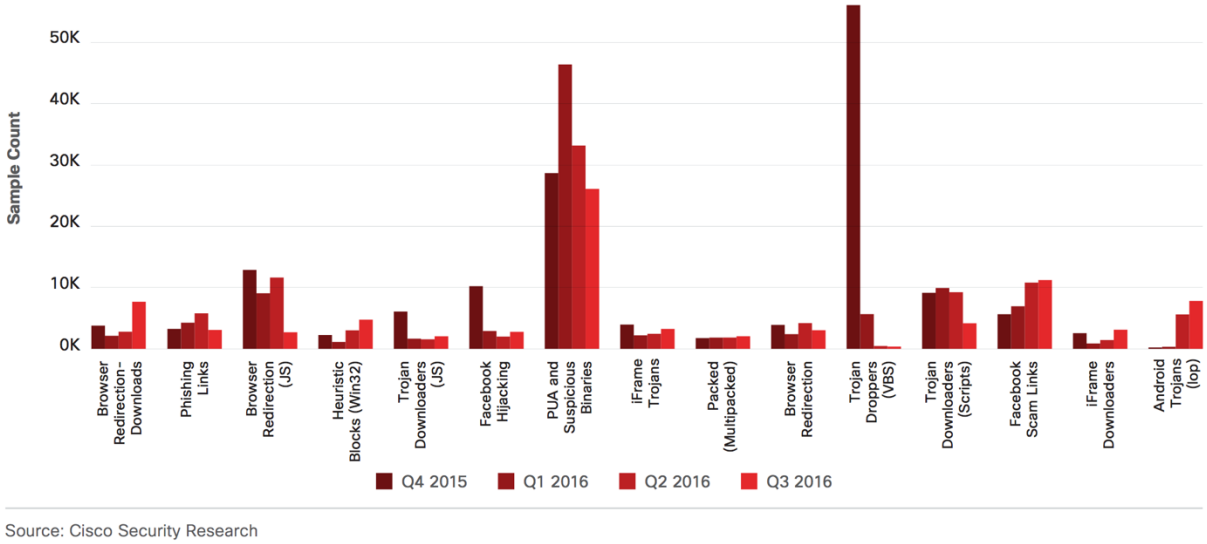
As we can see, it is very evident; adversaries are attempting to hack into all compute infrastructures starting from personal computer, mobile phones and all the way to datacenters and cloud servers. We understand the urgency in responding to security concerns that arise from Known (Insider)

ST Electronics (Info-Security) Pte. Ltd.
100 Jurong East Street 21, Singapore 609602
T: (65) 6568 7118 F: (65) 6568 7226
(Regn. No.: 199902746G)

and Unknown (Outsider) attacks and can provide technology solutions that are aimed at tackling such issues.

RECENT TRENDS

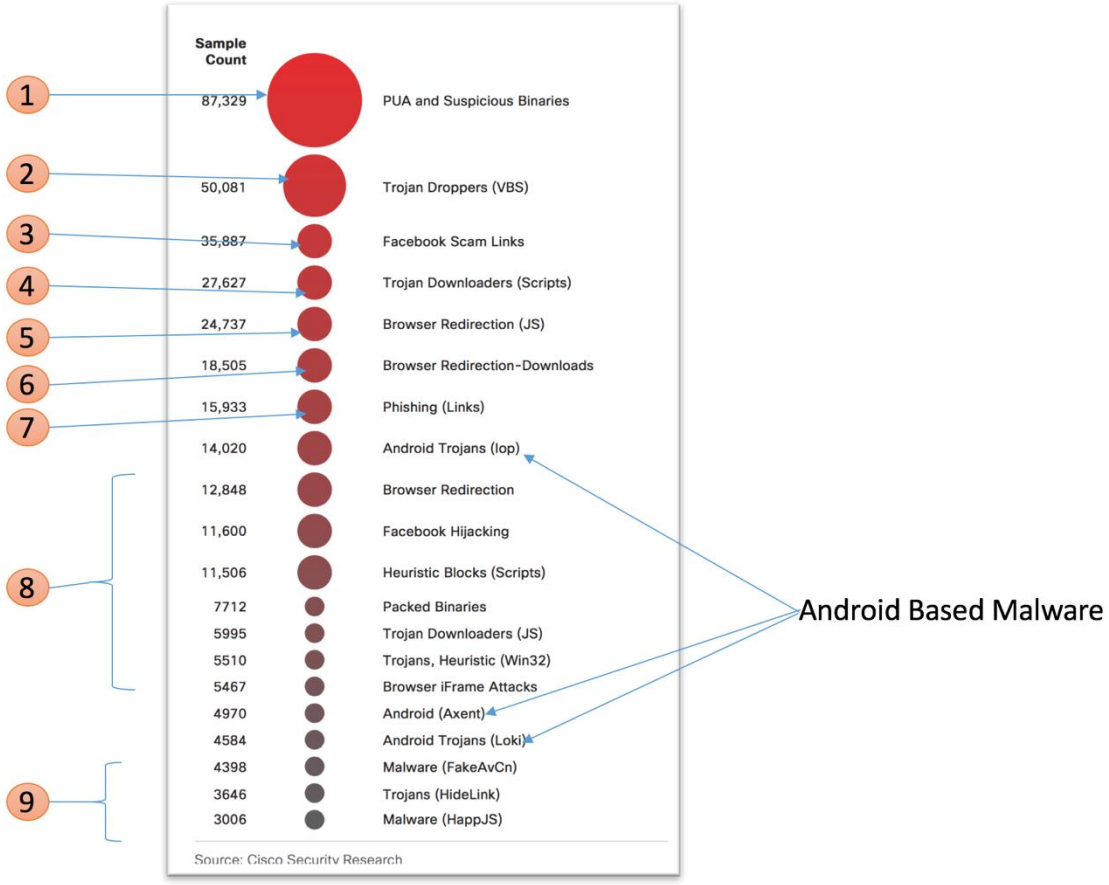
The recent trends below list how we can roughly categorise malware infections. Potentially Unknown Applications (PUAs) are the number one cause of network intrusion.



Source: Cisco Security Research

ST Electronics (Info-Security) Pte. Ltd.
100 Jurong East Street 21, Singapore 609602
T: (65) 6568 7118 F: (65) 6568 7226
(Regn. No.: 199902746G)

Here is a sample count of malware found in 2016, categorised by most to least occurrence.

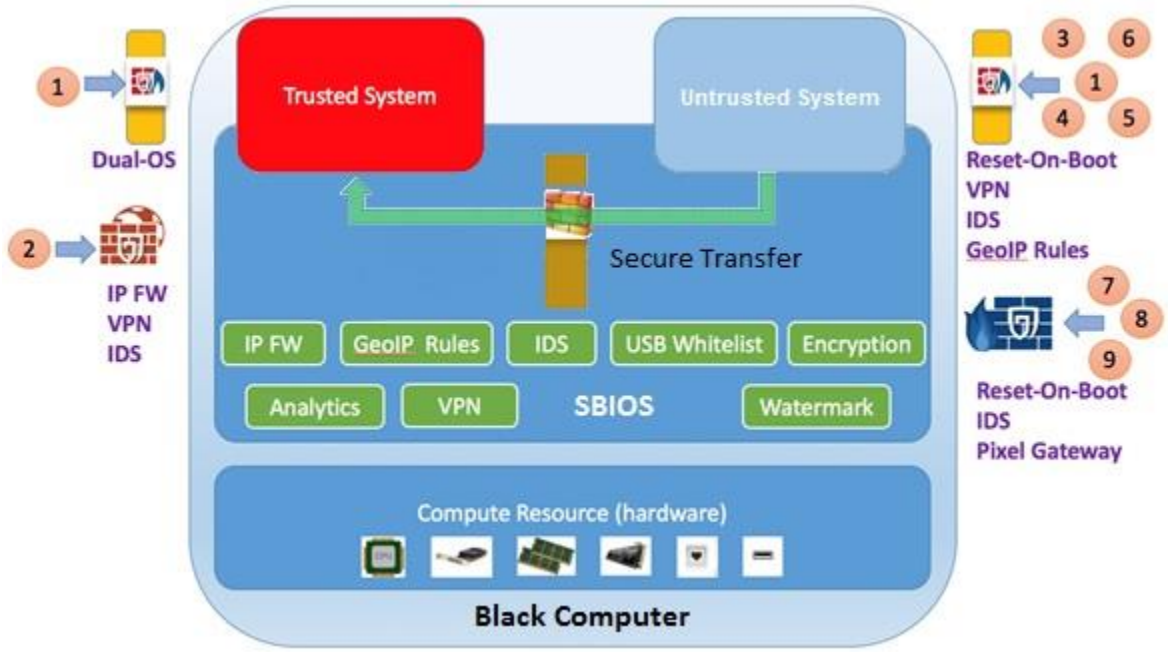


The list above is indexed with numbers, whichwill be used to match against the Black Computer's computer resource protection features.

ST Electronics (Info-Security) Pte. Ltd.
100 Jurong East Street 21, Singapore 609602
T: (65) 6568 7118 F: (65) 6568 7226
(Regn. No.: 199902746G)

BLACK COMPUTER FEATURES

Adopting a layered approach is essential when it comes to tackling security issue. Every layer enhances the defence mechanism against well-known attacks but no one layer should exist on its own. Black Computer implements Secure BIOS (SBIOS). The main difference between regular BIOS and SBIOS is that it takes in security features in software like IP-based firewall, GeoIP-based fencing and an Intrusion Detection System (IDS) to alert any unwanted network traffic. In the hardware layer, Trusted and Untrusted workspace are securely segregated with physical network separation.



The above diagram roughly depicts how Black Computer's features can provide defence against the list of well-known threats in the previous section. The following section describes how the Black Computer solution is applied to tackle these threats.

DEFENCE IN LAYERS

ST Electronics (Info-Security) Pte. Ltd.
100 Jurong East Street 21, Singapore 609602
T: (65) 6568 7118 F: (65) 6568 7226
(Regn. No.: 199902746G)

This section discusses the threats (1) to (9) that were listed in the section RECENT TRENDS.

PUA AND SUSPICIOUS BINARIES

PUA and suspicious binaries are nothing but Windows executables that are downloaded either by visiting malicious websites or inserting a USB that was infected via a worm/virus. Defence against these attacks should be implemented in a layered approach.

1. With dual-OS, Trusted and Untrusted workspaces are isolated as separate OS instances. A proprietary protocol – Secure Transfer – sits inside the Black Computer, which is a digital mirroring technique that filters all communications from the Untrusted workspace to the Trusted workspace. This helps to isolate attack surfaces that are exposed to network adversaries.
2. Trusted workspace is only allowed to connect to a Trusted network (Local LAN, Corporate LAN, etc.). By enforcing this, the Black Computer ensures the Untrusted workspace (that has access to Internet) will never be able to traverse through Secure Transfer to gain access to the Trusted workspace.
3. The Black Computer's Reset-On-Boot feature enables the Untrusted workspace to revert back to its golden state at every reboot, essentially making the Untrusted workspace instance like a Use-and-Throw instance.
4. GeoIP rules, VPN and IDS features can be implemented to fine tune how Untrusted workspace can access the Internet, making it harder for network adversaries to get to the Trusted workspace and its resources.

TROJAN DROPPERS

Trojan droppers are malware that are generally hidden to appear as either Microsoft Excel macro, or a crafted PDF file, or even a special DOCX template, etc. Black Computer's Secure Transfer feature prevents such macros from propagating into the Trusted workspace. In the event a user clicks on a malicious link in an email that was sent in the Trusted workspace, the Black Computer can prevent opening of such malicious links in the Trusted workspace. Instead, the link will pushed to the Untrusted workspace to be opened. If any malware or any trojan is present, the Black Computer will quarantine it to the Use-And-Throw instance and stop the propagation of the infection. The powerful IDS and IP firewall features can be used to alert IT administrator about unwanted connections into the system.

FACEBOOK SCAM LINKS

ST Electronics (Info-Security) Pte. Ltd.
100 Jurong East Street 21, Singapore 609602
T: (65) 6568 7118 F: (65) 6568 7226
(Regn. No.: 199902746G)

Facebook scam links are application level hijacking attacks that are cleverly crafted through Facebook posts that dupe users to click on malicious links. The Black Computer's Reset-On-Boot, Secure Transfer, IDS and IP firewall features prove to be an invaluable toolset to defend against these kind of attacks.

TROJAN DOWNLOADERS

Trojan downloaders are scripts that are executed after an infection. They form the connection back to their command and control servers. Technologies like VPN, IP firewall, IDS and Reset-On-Boot features prove as powerful defence.

BROWSER REDIRECTION / BROWSER REDIRECTION – DOWNLOADS

In general, these are due to DNS hijacking where malicious malware rewrites DNS entries and dupes users in opening malicious websites when the user intended to open legitimate URLs. These attacks can be detected by the Black Computer's IDS feature. In addtion, the VPN and IP firewall features can be used to allow and block connections that go through.

PHISHING (LINKS) / HEURISTIC BLOCKS / PACKED BINARIES

Such attacks are typically piggy-backed via an email or an attachment in an email that resembles legitimate URL. When the URL is clicked, the user is forced to visit unwanted websites that would result in downloading of Trojan binaries. Firstly, the IDS would inform the IT administrator of such malicious connections. Secondly, the Black Computer's Secure Transfer would limit the attack surface to Untrusted workspace. Lastly, the Reset-On-Boot feature destroys any malicious software that would have been deployed by visiting a malicious link. Tools like IDS and VPN can also be used to fine tune any connections going out of the Black Computer.

BROWSER IFRAME ATTACKS / MALWARE/ FAKE AV UPDATES

Browser attacks, similar to the phishing attacks, are generally caused by human error (users clicking on unwanted or malicious link). Features like Secure Transfer, IDS, VPN and Reset-On-Boot will help protect and limit, if not, isolate the attack.

ST Electronics (Info-Security) Pte. Ltd.
100 Jurong East Street 21, Singapore 609602
T: (65) 6568 7118 F: (65) 6568 7226
(Regn. No.: 199902746G)

www.stengg.com

The Black Computer supports remote monitoring to very detailed components – both in software and hardware, and is litigation-friendly. This allows the Black Computer to act like sensors for the Security Operation Centre to detect intrusions quicker, respond to it and minimise any damage.

The Remote Management System provides detail device management capability and remote control systems (reboot, shutdown, firmware, policy upgrade). This allows organisation to have the flexibility in deploying the Black Computer.

The Inspection System, which captures keystrokes, mouse clicks, and screen activities can be used for post-forensic and assist the administrators to quickly identify the source of intrusion. Irregularities and anomalies can be detected to alert the administrators of possible insider threats.

The Black Computer with its Inspection System and Remote Management System is a unique security solution to cover all threat aspects through segregated workspaces and its built-in security features to provide full protection coverage for the organisations.

ST Electronics (Info-Security) Pte. Ltd.
100 Jurong East Street 21, Singapore 609602
T: (65) 6568 7118 F: (65) 6568 7226
(Regn. No.: 199902746G)

CONCLUSION

While there is no system that can be considered perfectly secured, our Black Computer solution offers a layered approach to security that has proven to be the most effective way to prevent unwanted network intrusions by adversaries. We complement organisations' networks by bringing in the layered security starting from the endpoint, all the way to remote management and inspection system to monitor users and identify insider threats.

ST Electronics (Info-Security) Pte. Ltd.
100 Jurong East Street 21, Singapore 609602
T: (65) 6568 7118 F: (65) 6568 7226
(Regn. No.: 199902746G)