CYBERDEFENSES

Modern Cybersecurity

From Account Hijacking to Zero Days

Monty St John, May 2018

Modern Cybersecurity

Monty St John

Who is this guy?

- 25 years of security and analytics – physical, investigations, information, computer forensics, reverse engineering, threat intelligence
- Two decades supporting federal, state, and local LE while in uniform

Forensics and Threat Intelligence

- Better part of past decade acting as a key member of forensic and TI teams deconstructing, analyzing and providing insights into threats and how to thwart them

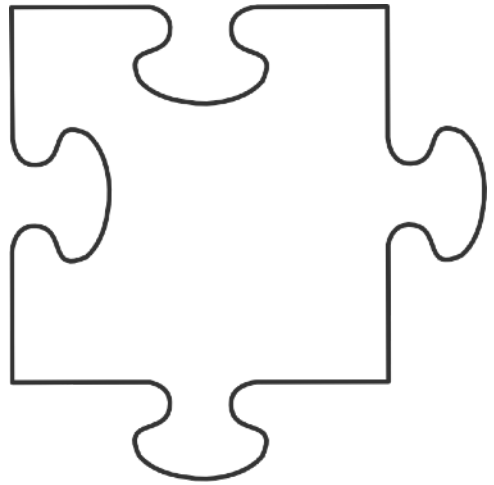
CYBERDEFENSES

Modern Cybersecurity

Digital Security == InfoSecurity == Cybersecurity

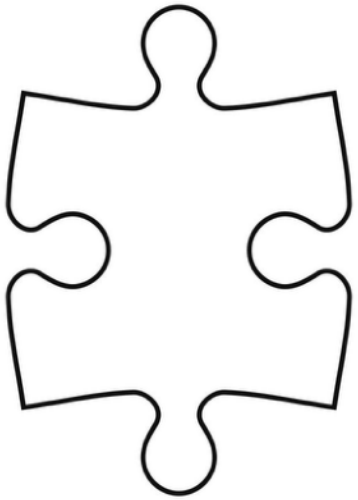
CYBERDEFENSES

Modern Cybersecurity



Data Security ≠ Cybersecurity

Its a differently shaped piece of the puzzle that happens to be a child of cybersecurity.



Modern Cybersecurity

Definition 1:

Cyber security is the practice of ensuring the integrity, confidentiality and availability (ICA) of information. It represents the ability to defend against and recover from accidents like hard drive failures or power outages, and from attacks by adversaries. It also includes everyone from insiders to outside adversaries.

Modern Cybersecurity

Most people rearrange that to be confidentiality. integrity and availability, or CIA.

If you have a CISSP or similar cert, you probably know this definition.

Modern Cybersecurity

Definition 2:

Cybersecurity is the protection of computer systems and networks from the theft and damage to their hardware, software or data, as well as from disruption, denial or misdirection of the services they provide.

Cybersecurity includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data, code injection, or through the careless or intentional actions of users.

Modern Cybersecurity

A much broader definition with a more defensive focus.

Modern Cybersecurity

Definition 3:

Cybersecurity is the techniques of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation.

Modern Cybersecurity

A little more limited in scope but still about protecting from the unauthorized or malicious.

Modern Cybersecurity

Six “Efforts” or functions of Cybersecurity

1. Detect
2. Investigate
3. Mitigate
4. Fix
5. Report
6. Educate

Modern Cybersecurity

Alert, discover, etc., all pretty much fall into the same bucket.

This is finding the pattern of activity or chain of execution that gives away something undesired or unexpected is occurring.

Modern Cybersecurity

Think:

- Digging in PCAPs to observe activity in network traffic
- Automated discovery or detection
- Customer/employee alerting to an issue
- Observations on activity
- Historical research or experience

Modern Cybersecurity

Investigate, or research, is exactly what it sounds like.

Here, you hunt, passively and actively, in the information you have, to find and define threats to security.

Investigate is also where you put the evidence to the actions, proving an event or execution occurred.

Modern Cybersecurity

Think:

- Researching exploits, adversaries, and malware
- Hunting within the enterprise for threats
- Investigating unusual events, anomalies and discrepancies from baseline to reality
- Employing intelligence to find threats, undetected activity or suspect actions.

Modern Cybersecurity

Mitigation or controls are the prevention and deterrence portions of cybersecurity.

These are the strategies and tactical moves made to reduce the chance of security issues and reduce their impact when they occur.

Modern Cybersecurity

Think:

- Creating layers of security, both ingress and egress
- Employing one type of application over another, to control potential data loss or enterprise impact
- Patching cadence
- Security inputs into business decisions
- Pre-emptive provision, removal or adjustment of assets

Modern Cybersecurity

While it seems obvious, fixing the problem is critical.

In the bustle and crisis of many incidents, controlling the incident happens quickly but actually instituting a fix tends to take time.

Modern Cybersecurity

Think:

- Adjusting security layers to cover a previously unknown or new part of the enterprise
- Shoring up a shortfall of intelligence, security, or tools
- Modernizing aging applications and architecture
- Chasing decision making to incorporate better information or streamlining to remove obstacles to better risk decisions

Modern Cybersecurity

A key element to good decision making is having the right information.

Reporting is providing that information, on direct, indirect and sometimes completely oblique threats.

Modern Cybersecurity

Think:

- Intelligence, Forensic and Security reports
- Threat landscape observations
- Shadow Market activity reports
- Competitor and Partner threat and risk reporting
- Analysis on current and past events

Modern Cybersecurity

Security is greater than acting like a fire department.

Response is a core function but only in teaching the enterprise can you prevent repeats of problems, excessive risk taking or poor decision making.

Modern Cybersecurity

Think:

- Guiding decision makers to make better informed decisions
- Training enterprise users in security hygiene
- Educating decision makers on what risks, security issues, and current events to watch
- Better informed decisions on purchases, acquisitions, mergers, etc.

Modern Cybersecurity

Welcome to the halfway point

source: gbttc.info/powerpoint-comic/powerpoint-comic-dilbert-on-powerpoint-slidegenius-presentation-agency/

Modern Cybersecurity

Account Takeover

A form of ID theft, where a 3rd party gains access to a trusted user's account. By posing as them, they can make changes, purchases, withdraw funds or contact other people.

source: www.creditcards.com/credit-card-news/account-takeover-fraud-rising.php

Modern Cybersecurity

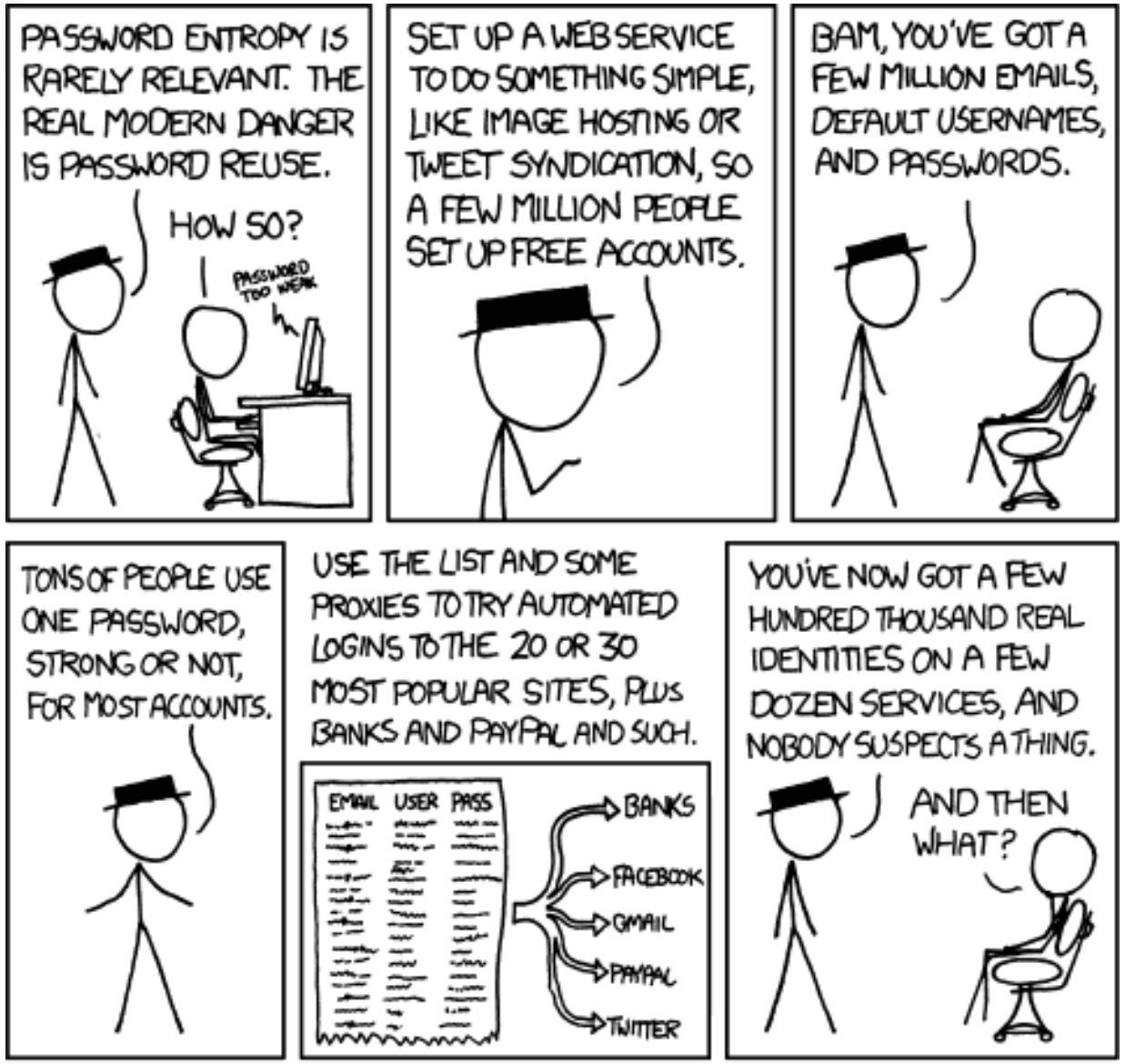
How significant is that?

Radicati's 2018 Study shows that 281.1B emails will be sent this year from a staggering 3.8B users. A person, on average, has 1.8 (really!?!) email accounts.

CDI's Spycloud service holds 9B unique credentials, since it began collecting in 2012. In our internal studies, an average person has 4 accounts between work and personal sources.

Source: www.radicati.com/wp/wp-content/uploads/2018/01/Email_Statistics_Report,_2018-2022_Executive_Summary.pdf

Modern Cybersecurity



Source: https://xkcd.com/792/

CYBERDEFENSES

Modern Cybersecurity

Application Shimming

A small library that transparently intercepts an API, changes the parameters passed, handles the operation itself, or redirects the operation elsewhere, such as additional code stored on a system.

Today, shims are mainly used for compatibility purposes for legacy applications. While shims serve a legitimate purpose, they can also be used in a malicious manner.

source: blog.externetworks.com/cyber-gang-robbed-100-banks-worldwide-did-they-even-breach-the-us-banks/

Modern Cybersecurity

BIGBADABOOM-2: BRAND NEW BREACH (TR2+TR1 DUMPS) at JOKER's STASH

BIGBADABOOM-2: BRAND NEW BREACH (TR2+TR1 DUMPS)

CHINA,AUSTRALIA,MEXICO,NEW ZEALAND,BRAZIL,TURKEY,FRANCE,SOUTH AFRICA,ITALY,GERMANY,
JAPAN,HONG KONG,UNITED ARAB EMIRATES,INDIA,SPAIN,NORWAY,SWEDEN,DENMARK,KOREA,ARGENTINA,
SWITZERLAND,SAUDI ARABIA,NETHERLANDS,ISRAEL,PORTUGAL,OMAN,BELGIUM,THAILAND,KUWAIT, ...

Another nick for Carbanak is JokerStash, who posted this sale of 5M credit cards.

These were later attributed as Saks 5th Ave and Lords & Taylor cards.

Modern Cybersecurity

source: www.makeuseof.com/tag/bootkit-nemesis-genuine-threat/

Bootkit

A boot-level rootkit that replaces or modifies the legitimate boot loader to be loaded before the operating system, and thus subvert any detect and destroy programs.

Modern Cybersecurity

Nemesis

Malware that attacks banks, payment card processors and other financial services.

We assisted a small financial institution with a security assessment. During that activity, we came across Nemesis in all kinds of places.

source: www.makeuseof.com/tag/bootkit-nemesis-genuine-threat/

Modern Cybersecurity

Brandjacking

Acquiring or assuming an online identity in order to acquire a person or business's brand equity.

Combines "branding" and "hijacking".

Modern Cybersecurity

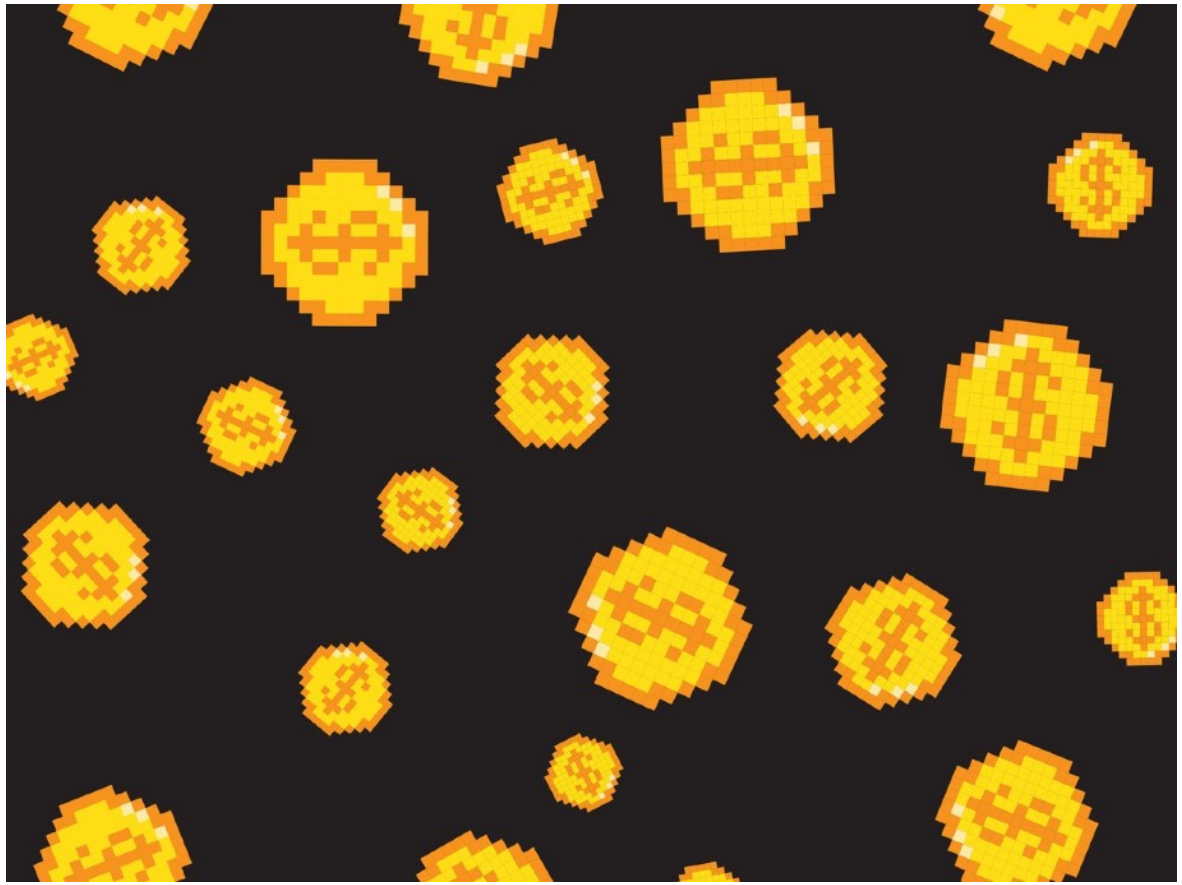
Source: https://twitter.com/hashtag/brandjacking

Modern Cybersecurity

Cryptojacking, Coinjacking

Browser Mining

Code/software that secretly uses your laptop or mobile device to mine cryptocurrency when you visit an infected site.



source: www.wired.com/story/cryptojacking-cryptocurrency-mining-browser/

Modern Cybersecurity

Remember this ???

Noah Dinkin, the CEO of stensul — an email marketing company —

> Hi @Starbucks @StarbucksAr did you know that your in-store wifi provider in Buenos Aires forces a 10 second delay when you first connect to the wifi so it can mine bitcoin using a customer's laptop? Feels a little off-brand.. cc @GMFlickinger pic.twitter.com/VkVVdSfUtT
>
> — Noah Dinkin (@imnoah) December 2, 2017

source: dailybitcoin.news/content/starbucks-store-caught-mining-monero-customers-laptops-using-wi-fi

Modern Cybersecurity

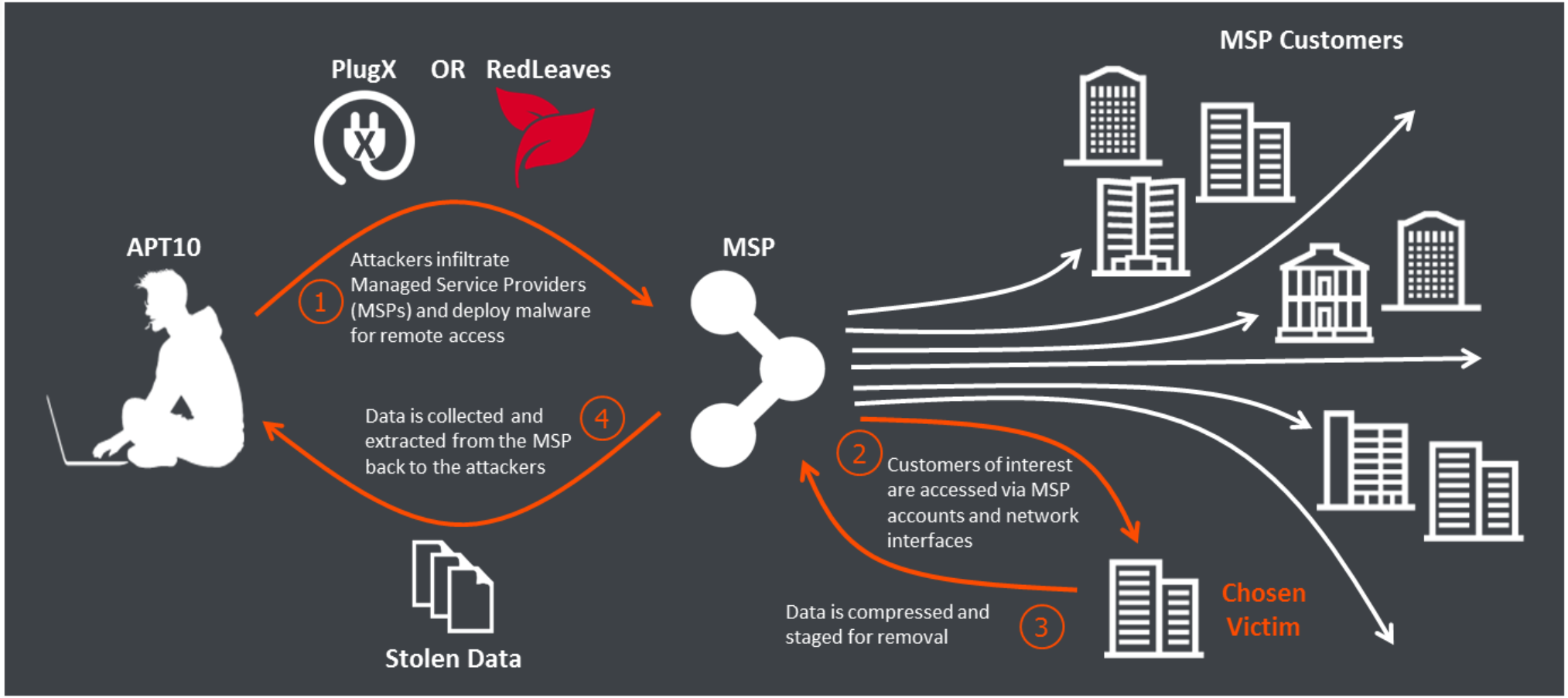
DLL search order hijacking

So what are the steps to perform a successful DLL hijacking attack?.

1. Target a certain application.
2. Monitor DLLs that are loaded by this application.
3. Find the search order for the DLLs
4. Target a DLL where you can put your malicious DLL to run before the legitimate DLL, or better target an unavailable DLL.
5. Find out which function this DLL is executing
6. Write a code you want to be executed when the DLL loads
7. Compile the code to shared library

source: http://www.bluekaizen.org/dll-hijacking-2/

Modern Cybersecurity



source: http://baesystemsai.blogspot.com/2017/04/apt10-operation-cloud-hopper_3.html

Operation focused on customers of or providers of Managed Services / Enterprise Service / Cloud Services

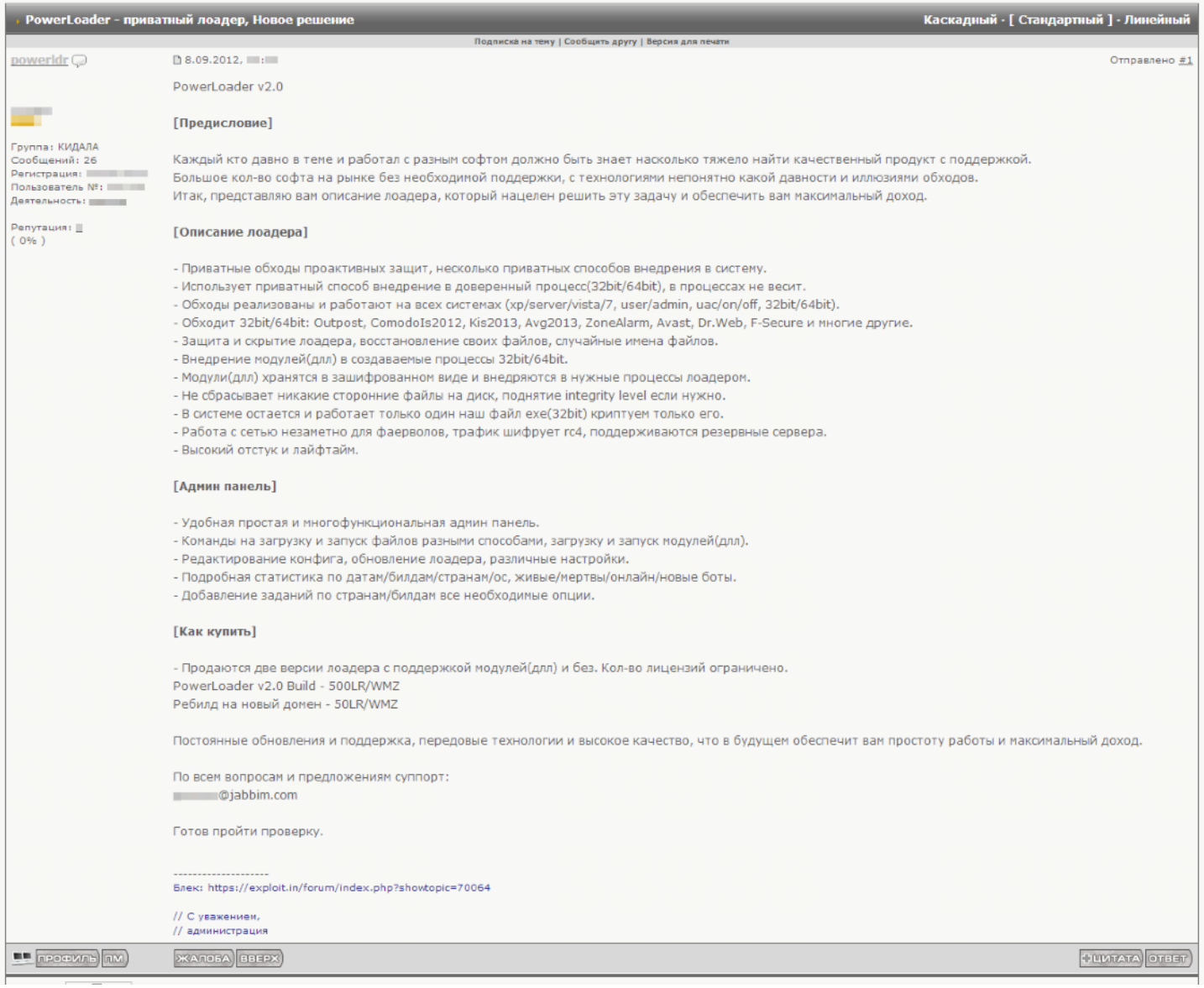
Modern Cybersecurity

Extra Window Memory Injection

Adding a little bit extra to find space to insert malware.

https://www.welivesecurity.com/2013/03/19/gapz-and-redyms-droppers-based-on-power-loader-code/

Modern Cybersecurity



PowerLoader - приватный лоадер, Новое решение

Каскадный - [Стандартный] - Линейный

Подписка на тему | Сообщить другу | Версия для печати

powerldr

8.09.2012,

Отправлено #1

Группа: КИДАЛА
Сообщений: 26
Регистрация:
Пользователь №:
Деятельность:

Репутация:
(0%)

PowerLoader v2.0

[Предисловие]

Каждый кто давно в теме и работал с разным софтом должно быть знает насколько тяжело найти качественный продукт с поддержкой.
Большое кол-во софта на рынке без необходимой поддержки, с технологиями непонятно какой давности и иллюзиями обходов.
Итак, представляю вам описание лоадера, который нацелен решить эту задачу и обеспечить вам максимальный доход.

[Описание лоадера]

- Приватные обходы проактивных защит, несколько приватных способов внедрения в систему.
- Использует приватный способ внедрение в доверенный процесс(32bit/64bit), в процессах не весит.
- Обходы реализованы и работают на всех системах (xp/server/vista/7, user/admin, uac/on/off, 32bit/64bit).
- Обходит 32bit/64bit: Outpost, ComodoIs2012, Kis2013, Avg2013, ZoneAlarm, Avast, Dr.Web, F-Secure и многие другие.
- Защита и скрытие лоадера, восстановление своих файлов, случайные имена файлов.
- Внедрение модулей(длл) в создаваемые процессы 32bit/64bit.
- Модули(длл) хранятся в зашифрованном виде и внедряются в нужные процессы лоадером.
- Не сбрасывает никакие сторонние файлы на диск, поднятие integrity level если нужно.
- В системе остается и работает только один наш файл exe(32bit) криптуем только его.
- Работа с сетью незаметно для фаерволов, трафик шифрует rc4, поддерживаются резервные сервера.
- Высокий отстук и лайфтайм.

[Админ панель]

- Удобная простая и многофункциональная админ панель.
- Команды на загрузку и запуск файлов разными способами, загрузку и запуск модулей(длл).
- Редактирование конфига, обновление лоадера, различные настройки.
- Подробная статистика по датам/билдам/странам/ос, живые/мертвы/онлайн/новые боты.
- Добавление заданий по странам/билдам все необходимые опции.

[Как купить]

- Продаются две версии лоадера с поддержкой модулей(длл) и без. Кол-во лицензий ограничено.
PowerLoader v2.0 Build - 500LR/WMZ
Ребилд на новый домен - 50LR/WMZ

Постоянные обновления и поддержка, передовые технологии и высокое качество, что в будущем обеспечит вам простоту работы и максимальный доход.

По всем вопросам и предложениям суппорт:
@jabbim.com

Готов пройти проверку.

Блек: https://exploit.in/forum/index.php?showtopic=70064

// С уважением,
// администрация

ПРОФИЛЬ ЛМ ЖАЛОБА ВВЕРХ +ЦИТАТА ОТВЕТ

http://www.xylibox.com/2013/09/powerloader-20-alueron.html

Modern Cybersecurity

PowerLoader v2.0

[Preface]
Anyone who's in this business knows how difficult it is to find a good product with a good support.
Lots of software currently on the market is lack of the support and uses some ancient technologies with questionable bypass techniques.
So, here is the description of the loader that will solve these problems and increase your earnings.

[Loader Description]

- Private pro-active defences bypass code, includes a number of private OS integration methods.
- Uses private process attach method for (32bit/64bit), doesn't hang in the processes.
- Bypasses are implemented and working on all OS versions (xp/server/vista/7, user/admin, uac/on/off, 32bit/64bit)
- Successfully bypasses 32bit/64bit: Outpost, ComodoIs2012, Kis2013, Avg2013, ZoneAlarm, Avast, Dr.Web, F-Secure and many more.
- Protects and hides the loader, allows to restore your files, random filenames.
- Supports DLL injection in 32bit/64bit processes.
- DLLs are stored encrypted and injected into the processes by the loader.
- Doesn't store any leftover/rubbish files on the disk - integrity level.
- The only file that is left on the system and the only file working is your EXE(32bit), encrypting is done on that file only.
- Network activity is hidden from the firewalls, traffic is encrypted with RC4, supports backup servers.
- High callback rate and lifetime.

Modern Cybersecurity

[Admin Panel]
- Easy to use multifunctional admin panel.
- Provides different load and execute commands for different types of files including DLLs
- Configuration editing, loader update, many other settings.
- Detailed statistics by date/build/countries/OS, live/dead/online/new bots.
- Tasks assignment by countries/builds with all necessary options.

[How to buy]
- We sell two loader versions - with and without DLL support. Number of licences is limited.
PowerLoader v2.0 Build - 500LR/WMZ
Rebuild for a new domain - 50LR/WMZ
Constant updates and support, latest technologies and high quality that will provide you with easy operation and bring top earnings.
Please contact support if you have any questions:
....@jabbim.com
Ready to take any tests on.

Modern Cybersecurity

statSystem	Count* (% Now)	Average Life time **	% Dead/Month
5.1 2600 sp0.0 32bit	2 (0.05%) / 0 (0%) / 2 (0.05%) / 0 (0%)	24.92 д. / 39.67 д.	132.22%
5.1 2600 sp1.0 32bit	1 (0.03%) / 0 (0%) / 1 (0.03%) / 0 (0%)	1.51 д. / 13.98 д.	46.59%
5.1 2600 sp2.0 32bit	179 (4.74%) / 5 (0.13%) / 174 (4.61%) / 4 (0.11%)	8.45 д. / 37.19 д.	120.51%
5.1 2600 sp3.0 32bit	2341 (62.03%) / 59 (1.56%) / 2282 (60.47%) / 38 (1.01%)	7.24 д. / 38.16 д.	123.99%
5.2 3790 sp1.0 32bit	9 (0.24%) / 2 (0.05%) / 7 (0.19%) / 2 (0.05%)	20.71 д. / 39.84 д.	103.29%
5.2 3790 sp2.0 32bit	113 (2.99%) / 24 (0.64%) / 89 (2.36%) / 19 (0.5%)	20.84 д. / 38.32 д.	100.6%
6.0 6000 sp0.0 32bit	6 (0.16%) / 0 (0%) / 6 (0.16%) / 0 (0%)	7.19 д. / 39.83 д.	132.77%
6.0 6001 sp1.0 32bit	13 (0.34%) / 1 (0.03%) / 12 (0.32%) / 1 (0.03%)	10.2 д. / 34.06 д.	104.79%
6.0 6001 sp1.0 64bit	5 (0.13%) / 0 (0%) / 5 (0.13%) / 0 (0%)	11.98 д. / 33.36 д.	111.21%
6.0 6002 sp2.0 32bit	54 (1.43%) / 1 (0.03%) / 53 (1.4%) / 1 (0.03%)	5.79 д. / 35.58 д.	116.42%
6.0 6002 sp2.0 64bit	27 (0.72%) / 2 (0.05%) / 25 (0.66%) / 1 (0.03%)	7.26 д. / 37.35 д.	115.29%
6.1 7600 sp0.0 32bit	46 (1.22%) / 4 (0.11%) / 42 (1.11%) / 0 (0%)	7.29 д. / 37.74 д.	114.86%
6.1 7600 sp0.0 64bit	54 (1.43%) / 0 (0%) / 54 (1.43%) / 0 (0%)	6.25 д. / 34.21 д.	114.04%
6.1 7601 sp1.0 32bit	274 (7.26%) / 3 (0.08%) / 271 (7.18%) / 0 (0%)	5.33 д. / 37.17 д.	122.55%
6.1 7601 sp1.0 64bit	648 (17.17%) / 6 (0.16%) / 642 (17.01%) / 0 (0%)	4.6 д. / 35.18 д.	116.19%
6.2 9200 sp0.0 32bit	2 (0.05%) / 0 (0%) / 2 (0.05%) / 0 (0%)	2 д. / 39.3 д.	131%

*« bots / Alive / Dead / Online »

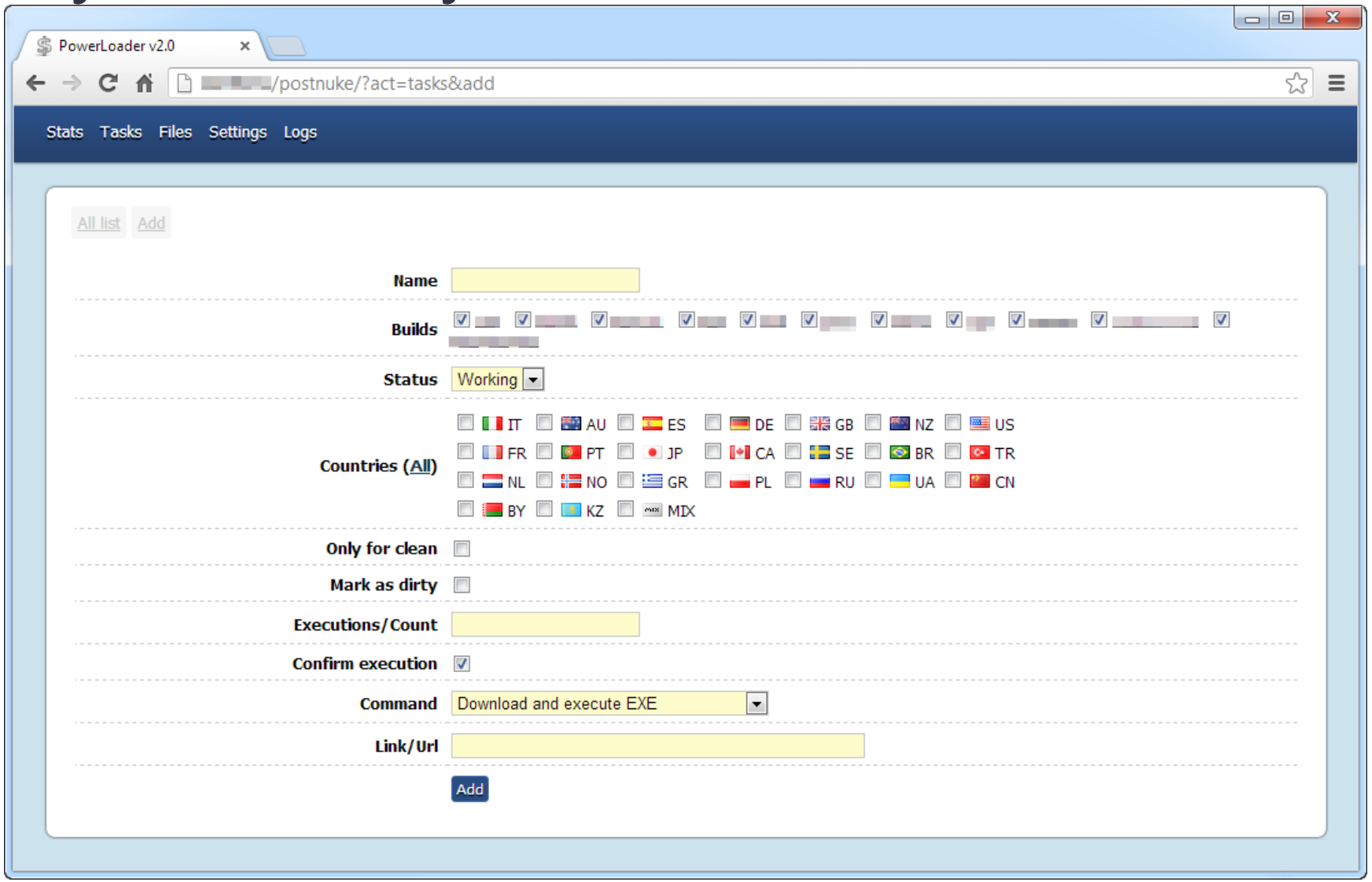
CYBERDEFENSES

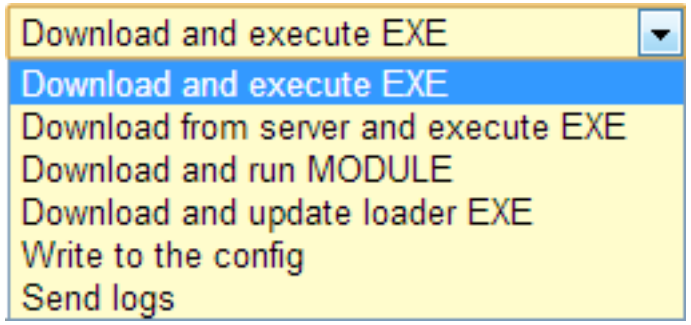
Modern Cybersecurity

statCountry	Count* (% Now)	Average Life time **	% Dead/Month
A1	1 (0.03%) / 0 (0%) / 1 (0.03%) / 0 (0%)	1.08 д. / 38.56 д.	128.54%
AE	11 (0.29%) / 0 (0%) / 11 (0.29%) / 0 (0%)	8.06 д. / 39.89 д.	132.95%
AN	1 (0.03%) / 0 (0%) / 1 (0.03%) / 0 (0%)	2.27 д. / 40.23 д.	134.1%
AO	1 (0.03%) / 0 (0%) / 1 (0.03%) / 0 (0%)	5.28 д. / 39.32 д.	131.05%
AP	1 (0.03%) / 0 (0%) / 1 (0.03%) / 0 (0%)	1.85 д. / 39.78 д.	132.6%
AT	2 (0.05%) / 0 (0%) / 2 (0.05%) / 0 (0%)	2.14 д. / 39.88 д.	132.94%
AU	7 (0.19%) / 0 (0%) / 7 (0.19%) / 0 (0%)	5.25 д. / 39.81 д.	132.7%
BE	13 (0.34%) / 0 (0%) / 13 (0.34%) / 0 (0%)	8.55 д. / 37.87 д.	126.24%
BG	1 (0.03%) / 0 (0%) / 1 (0.03%) / 0 (0%)	22.21 д. / 39.59 д.	131.98%
BR	3 (0.08%) / 1 (0.03%) / 2 (0.05%) / 0 (0%)	14.6 д. / 39.85 д.	88.55%
BY	1 (0.03%) / 0 (0%) / 1 (0.03%) / 0 (0%)	2.84 д. / 40.23 д.	134.11%
BZ	1 (0.03%) / 0 (0%) / 1 (0.03%) / 0 (0%)	6.03 д. / 40.35 д.	134.52%
CA	537 (14.23%) / 8 (0.21%) / 529 (14.02%) / 7 (0.19%)	7.29 д. / 38.61 д.	126.8%
CH	3 (0.08%) / 0 (0%) / 3 (0.08%) / 0 (0%)	3.43 д. / 40.03 д.	133.45%
CL	2 (0.05%) / 0 (0%) / 2 (0.05%) / 0 (0%)	1.6 д. / 40.21 д.	134.02%
CN	13 (0.34%) / 0 (0%) / 13 (0.34%) / 0 (0%)	4.55 д. / 35.25 д.	117.48%
CO	2 (0.05%) / 0 (0%) / 2 (0.05%) / 0 (0%)	1.26 д. / 39.21 д.	130.7%
DE	11 (0.29%) / 0 (0%) / 11 (0.29%) / 0 (0%)	1.77 д. / 39.54 д.	131.79%
DK	7 (0.19%) / 0 (0%) / 7 (0.19%) / 0 (0%)	1.23 д. / 39.99 д.	133.31%
DO	1 (0.03%) / 0 (0%) / 1 (0.03%) / 0 (0%)	1.27 д. / 39.23 д.	130.78%
EC	1 (0.03%) / 0 (0%) / 1 (0.03%) / 0 (0%)	3.41 д. / 38.8 д.	129.33%
EG	2 (0.05%) / 0 (0%) / 2 (0.05%) / 0 (0%)	14.36 д. / 40.17 д.	133.9%
ES	6 (0.16%) / 0 (0%) / 6 (0.16%) / 0 (0%)	3.16 д. / 34.56 д.	115.19%
EU	15 (0.4%) / 0 (0%) / 15 (0.4%) / 0 (0%)	1.87 д. / 40.23 д.	134.1%
FI	1 (0.03%) / 0 (0%) / 1 (0.03%) / 0 (0%)	5.84 д. / 40.34 д.	134.48%
FJ	1 (0.03%) / 0 (0%) / 1 (0.03%) / 0 (0%)	1.04 д. / 40.02 д.	133.38%
FR	16 (0.42%) / 0 (0%) / 16 (0.42%) / 0 (0%)	6.87 д. / 39.61 д.	132.02%
GB	106 (2.81%) / 1 (0.03%) / 105 (2.78%) / 0 (0%)	3.21 д. / 39.39 д.	130.07%
GR	2 (0.05%) / 0 (0%) / 2 (0.05%) / 0 (0%)	15.7 д. / 40.14 д.	133.8%
GT	1 (0.03%) / 0 (0%) / 1 (0.03%) / 0 (0%)	1.23 д. / 39.26 д.	130.86%
HK	2 (0.05%) / 0 (0%) / 2 (0.05%) / 0 (0%)	2.02 д. / 39.8 д.	132.68%
ID	5 (0.13%) / 0 (0%) / 5 (0.13%) / 0 (0%)	9.67 д. / 39.1 д.	130.34%
IE	9 (0.24%) / 1 (0.03%) / 8 (0.21%) / 0 (0%)	11.57 д. / 36.92 д.	109.4%
IL	6 (0.16%) / 0 (0%) / 6 (0.16%) / 0 (0%)	12.9 д. / 40.46 д.	134.88%
IN	41 (1.09%) / 2 (0.05%) / 39 (1.03%) / 0 (0%)	5.46 д. / 40.13 д.	127.23%
IQ	1 (0.03%) / 0 (0%) / 1 (0.03%) / 0 (0%)	22.12 д. / 39.65 д.	132.18%
IT	8 (0.21%) / 0 (0%) / 8 (0.21%) / 0 (0%)	1.97 д. / 39.97 д.	133.22%
JP	1 (0.03%) / 0 (0%) / 1 (0.03%) / 0 (0%)	1.67 д. / 39.59 д.	131.98%
KR	8 (0.21%) / 0 (0%) / 8 (0.21%) / 0 (0%)	5.55 д. / 38.31 д.	127.69%
KZ	1 (0.03%) / 0 (0%) / 1 (0.03%) / 0 (0%)	1.02 д. / 40.35 д.	134.52%
LK	1 (0.03%) / 0 (0%) / 1 (0.03%) / 0 (0%)	7.4 д. / 39.86 д.	132.87%
LT	4 (0.11%) / 1 (0.03%) / 3 (0.08%) / 0 (0%)	16.86 д. / 40.67 д.	101.67%
MA	1 (0.03%) / 0 (0%) / 1 (0.03%) / 0 (0%)	1.02 д. / 40.21 д.	134.04%
MD	1 (0.03%) / 0 (0%) / 1 (0.03%) / 0 (0%)	4.58 д. / 39.32 д.	131.05%
MT	1 (0.03%) / 0 (0%) / 1 (0.03%) / 0 (0%)	1.02 д. / 38.64 д.	128.79%
MX	7 (0.19%) / 1 (0.03%) / 6 (0.16%) / 0 (0%)	18.76 д. / 39.58 д.	113.09%
MY	3 (0.08%) / 0 (0%) / 3 (0.08%) / 0 (0%)	1.65 д. / 37.64 д.	125.47%
NL	12 (0.32%) / 0 (0%) / 12 (0.32%) / 0 (0%)	2.9 д. / 39.33 д.	131.09%
NZ	1 (0.03%) / 0 (0%) / 1 (0.03%) / 0 (0%)	4.99 д. / 39.94 д.	133.15%
OM	1 (0.03%) / 0 (0%) / 1 (0.03%) / 0 (0%)	7.01 д. / 40.02 д.	133.38%
PE	1 (0.03%) / 0 (0%) / 1 (0.03%) / 0 (0%)	1.03 д. / 37.2 д.	124.01%
PH	2 (0.05%) / 0 (0%) / 2 (0.05%) / 0 (0%)	10.03 д. / 38.95 д.	129.82%
PK	4 (0.11%) / 0 (0%) / 4 (0.11%) / 0 (0%)	4.73 д. / 39.52 д.	131.75%
PL	1 (0.03%) / 0 (0%) / 1 (0.03%) / 0 (0%)	1.16 д. / 39.69 д.	132.29%
PR	15 (0.4%) / 0 (0%) / 15 (0.4%) / 0 (0%)	2.93 д. / 38.45 д.	128.16%
PT	1 (0.03%) / 0 (0%) / 1 (0.03%) / 0 (0%)	1.88 д. / 39.96 д.	133.21%
PY	1 (0.03%) / 0 (0%) / 1 (0.03%) / 0 (0%)	1.76 д. / 40.18 д.	133.93%
QA	1 (0.03%) / 0 (0%) / 1 (0.03%) / 0 (0%)	1.22 д. / 39.74 д.	132.48%
RO	6 (0.16%) / 0 (0%) / 6 (0.16%) / 0 (0%)	1.62 д. / 37.98 д.	126.61%
RU	3 (0.08%) / 0 (0%) / 3 (0.08%) / 0 (0%)	21.4 д. / 35.45 д.	118.16%
SA	3 (0.08%) / 0 (0%) / 3 (0.08%) / 0 (0%)	10.62 д. / 39.03 д.	130.1%
SE	8 (0.21%) / 0 (0%) / 8 (0.21%) / 0 (0%)	2.49 д. / 39.84 д.	132.81%
SG	7 (0.19%) / 0 (0%) / 7 (0.19%) / 0 (0%)	3.14 д. / 39.17 д.	130.57%
SK	1 (0.03%) / 0 (0%) / 1 (0.03%) / 0 (0%)	1.02 д. / 39.29 д.	130.97%
SN	1 (0.03%) / 0 (0%) / 1 (0.03%) / 0 (0%)	1.31 д. / 39.21 д.	130.71%
TR	1 (0.03%) / 0 (0%) / 1 (0.03%) / 0 (0%)	1.51 д. / 38.63 д.	128.75%
TT	21 (0.56%) / 0 (0%) / 21 (0.56%) / 0 (0%)	2.72 д. / 39.92 д.	133.05%
TW	2 (0.05%) / 0 (0%) / 2 (0.05%) / 0 (0%)	2.39 д. / 39.86 д.	132.87%
UA	3 (0.08%) / 0 (0%) / 3 (0.08%) / 0 (0%)	4.09 д. / 29.12 д.	97.06%
UNKNOWN	1 (0.03%) / 0 (0%) / 1 (0.03%) / 0 (0%)	6.06 д. / 37.88 д.	126.25%
US	2789 (73.9%) / 92 (2.44%) / 2697 (71.46%) / 59 (1.56%)	7.45 д. / 36.91 д.	118.99%
VE	2 (0.05%) / 0 (0%) / 2 (0.05%) / 0 (0%)	3.03 д. / 40.18 д.	133.94%
VI	1 (0.03%) / 0 (0%) / 1 (0.03%) / 0 (0%)	26.11 д. / 40.24 д.	134.12%
VN	4 (0.11%) / 0 (0%) / 4 (0.11%) / 0 (0%)	11.12 д. / 29.2 д.	97.34%
ZA	11 (0.29%) / 0 (0%) / 11 (0.29%) / 0 (0%)	2.22 д. / 39.2 д.	130.66%

* « bots / Alive / Dead / Online »

Modern Cybersecurity





Modern Cybersecurity

"From: Alice"
(really is from Eve)

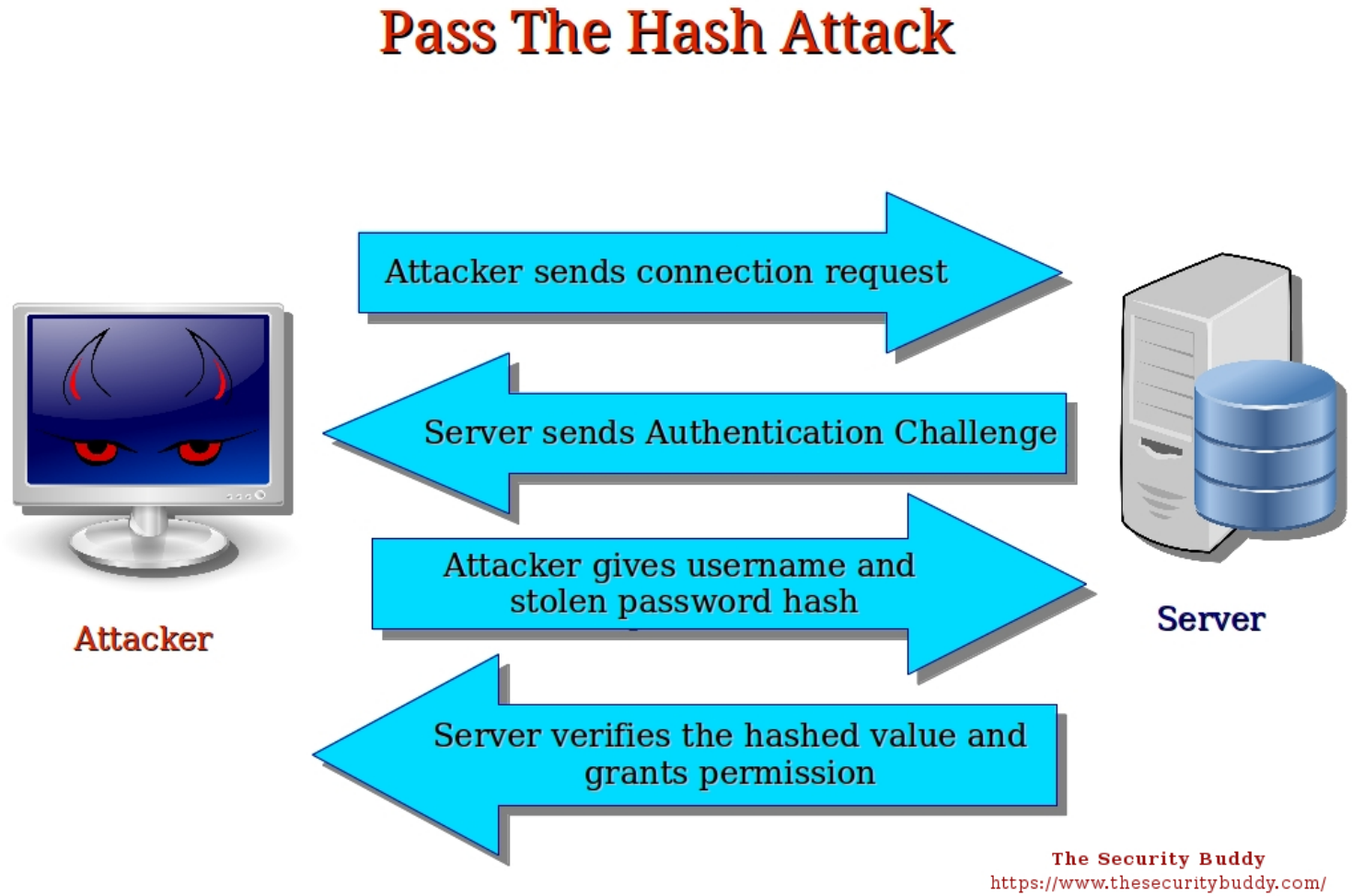
Masquerading

When the name or location of an executable, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation.

Modern Cyber

Pass the Hash

A way of authenticating as a user without having access to the user's cleartext password.



Modern Cybersecurity

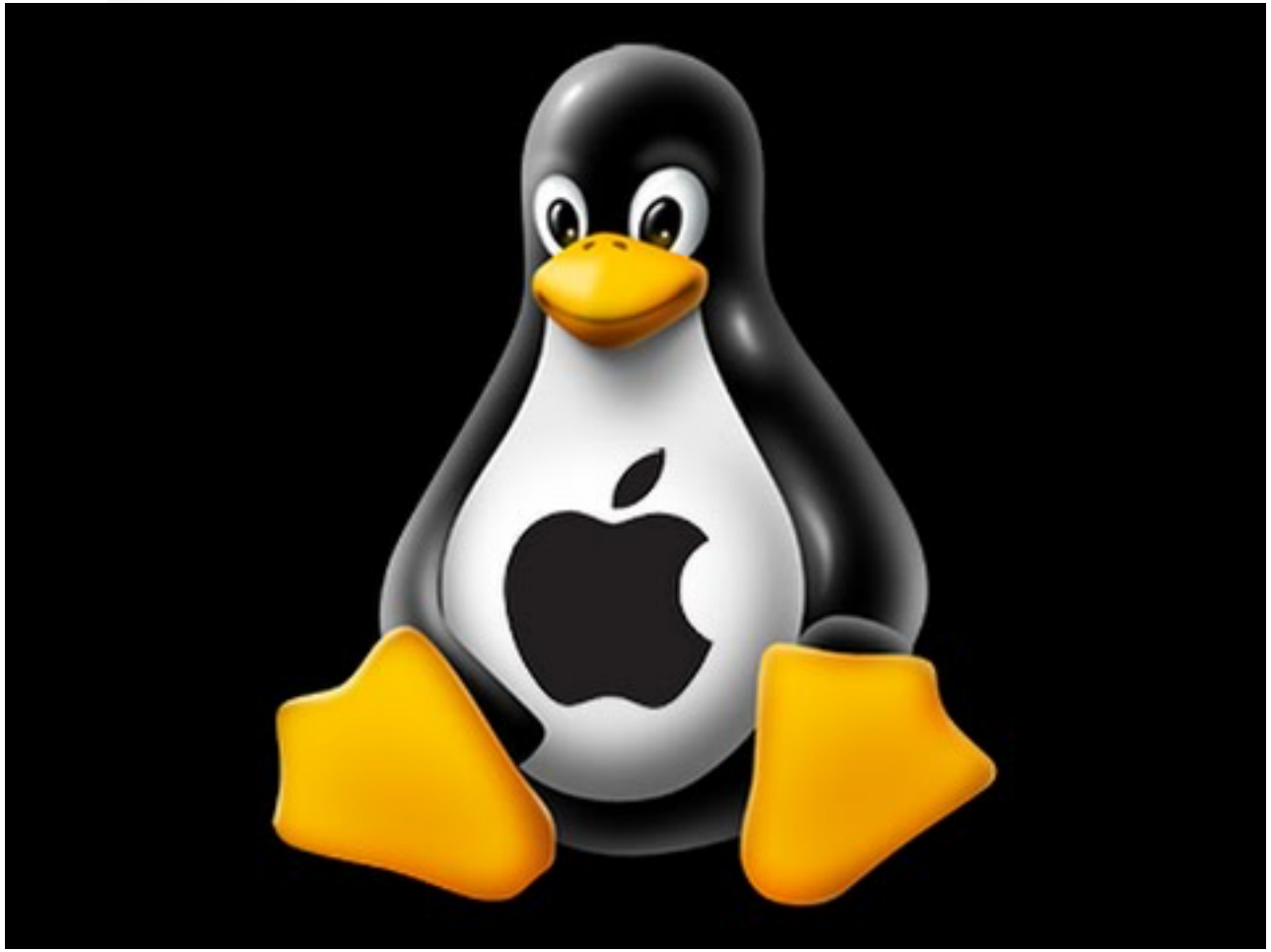
Port Knocking

Port knocking is a stealth method to externally open ports that, by default, the firewall keeps closed.

It works by requiring connection attempts to a series of predefined closed ports. When the correct sequence of port "knocks" (connection attempts) is received, the firewall opens certain port(s) to allow a connection.

source: blog.trendmicro.com/trendlabs-security-intelligence/pokemon-themed-umbreon-linux-rootkit-hits-x86-arm-systems/

Modern Cybersecurity



I know we are talking about a lot of Windows based issues and malware but … the Umbreon Rootkit only works on Mac and Linux…and its really, really hard to detect.

Modern Cybersecurity

Process Doppelgänging

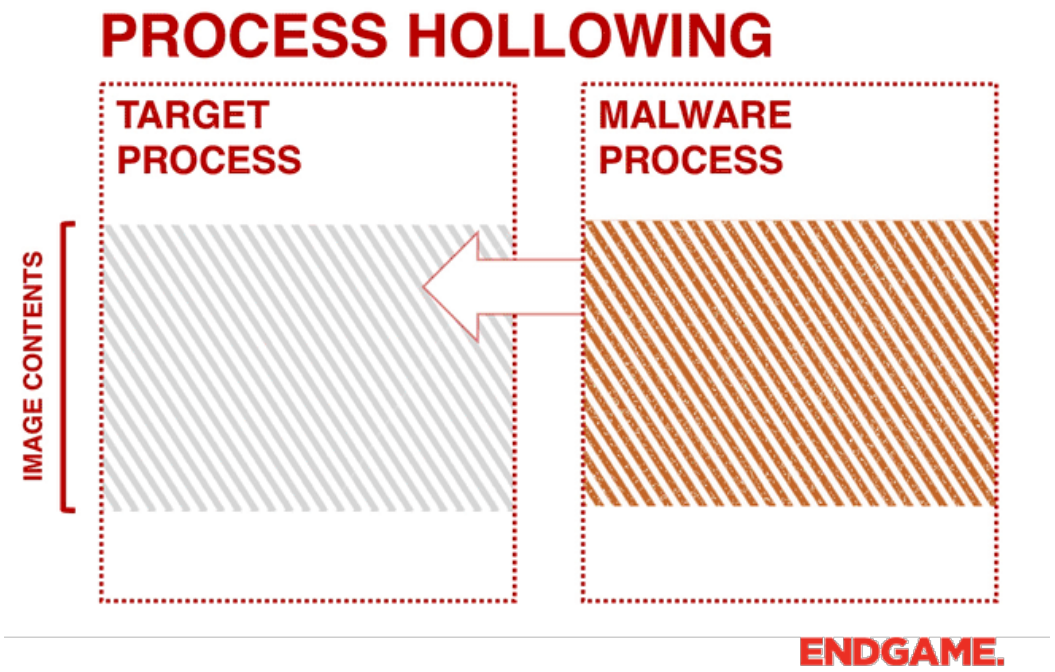
source: www.hackread.com/process-doppelganging-attack-windows-evades-av/

The ability to run a malicious executable under the cover of a legitimate one. In short, it creates a file inside a transaction, making the file is invisible to all other processes, as long as our transaction is not committed.

It can be used to drop and run malicious payloads in an unnoticed way. If we roll back the transaction in an appropriate moment, the operating system behaves like our file was never created.

Modern Cybersecurity

Process Hollowing



source: www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process

A technique used by malware in which a legitimate process is loaded on the system solely to act as a container for hostile code.

At launch, the legitimate process is created in a suspended state and the process's memory is replaced with the code of a second program so that the second program runs instead of the original.

Modern Cybersecurity

Duqu, one of the “four brothers” of highly sophisticated, probably truest “nation-state” espionage toolsets currently discovered.

Eventually linked to US & Israeli espionage activity

source: www.ibtimes.co.uk/duqu-2-most-advanced-cyber-espionage-tool-ever-discovered-1505439

Modern Cybersecurity

Whaling

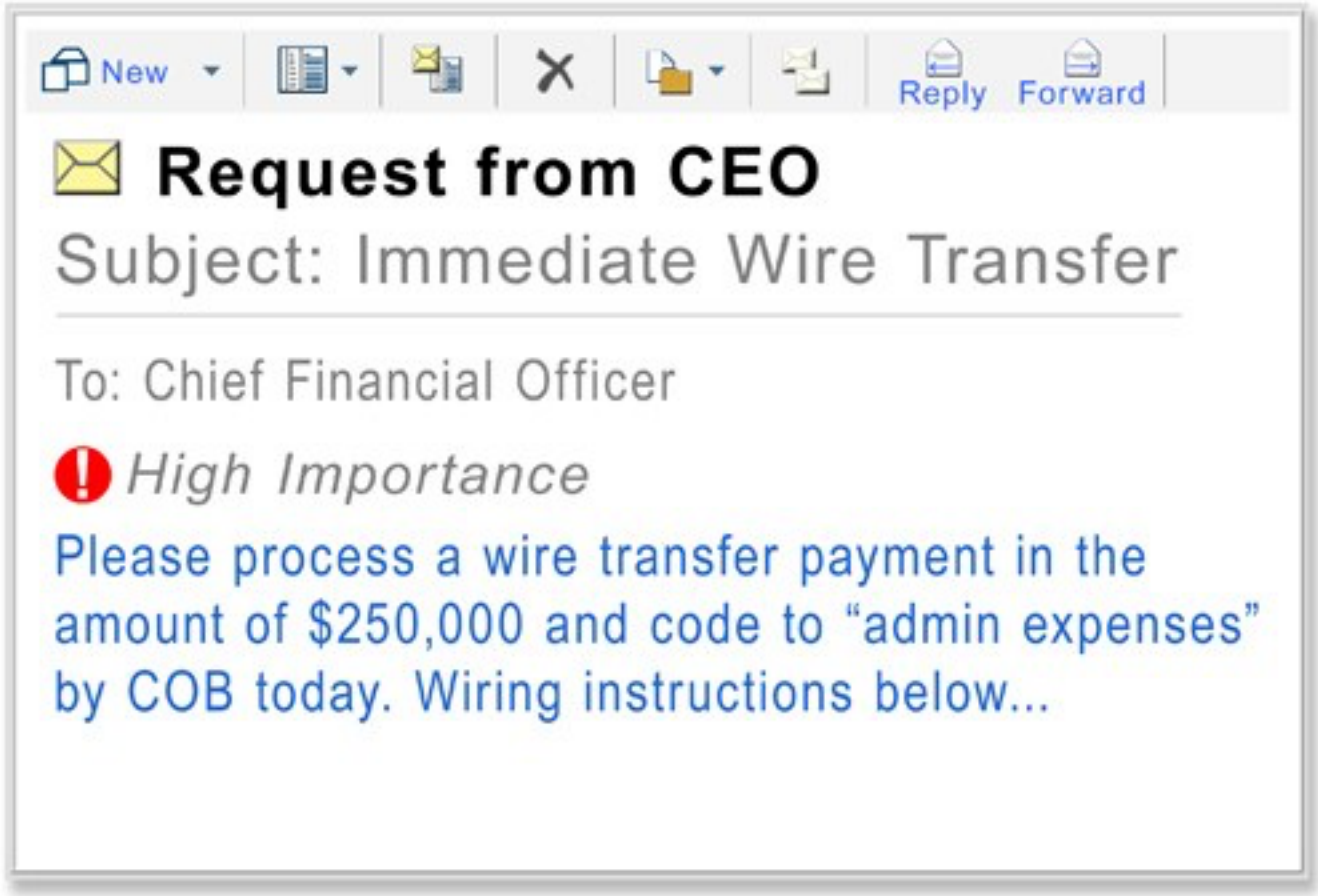
Spearphishing against your CEO

72%

of whaling attackers pretended to be the CEO, while 36% were attributed to the CFO.

source: www.thewindowsclub.com/what-are-whaling-scams

Modern Cybersecurity



Modern Cybersecurity

An attack that **exploits** a previously unknown security vulnerability.

A **zero-day** attack is also sometimes defined as an attack that takes advantage of a security vulnerability on the same **day** that the vulnerability becomes generally known.

Modern Cybersecurity

Gamma Group International - Selling “legal” malware. UK-based surveillance company that sells malware called “FinFisher” to repressive regimes (and anyone else). It is sold as "governmental IT intrusion and remote monitoring solutions" and operates in at least 36 countries.

Hacked in 2014 and a 40 Gb dump of information was released detailing Gamma's 'client lists, price lists, source code, details about the effectiveness of FinFisher malware, user and support documentation, a list of classes/tutorials, and much more.

Modern Cybersecurity

FinFisher employs numerous zero-days to gain a foothold and download its malware.

Most common is via Word or Hangul exploits.

Files and Slides

https://github.com/CyberDefenses/Conventions

Cybersecurity Fundamentals

Questions?

Twitter: @montystjohn
LinkedIn: www.linkedin.com/in/monty-st-john-3842692
Github: github.com/corumir
CDI Github: github.com/cyberdefenses

CYBERDEFENSES

THANK YOU

1205 Sam Bass Rd. Suite 300 Round Rock, TX 78681

512-255-3700 • info@cyberdefenses.com • www.cyberdefenses.com