KASPERSKY®

ATM: EVERY DAY TROUBLE

ALL CHARACTERS AND EVENTS IN THIS SHOW--EVEN THOSE BASED ON REAL PEOPLE--ARE ENTIRELY FICTIONAL.

ALEXEY OSIPOV, OLGA KOCHETOVA KASPERSKY LAB

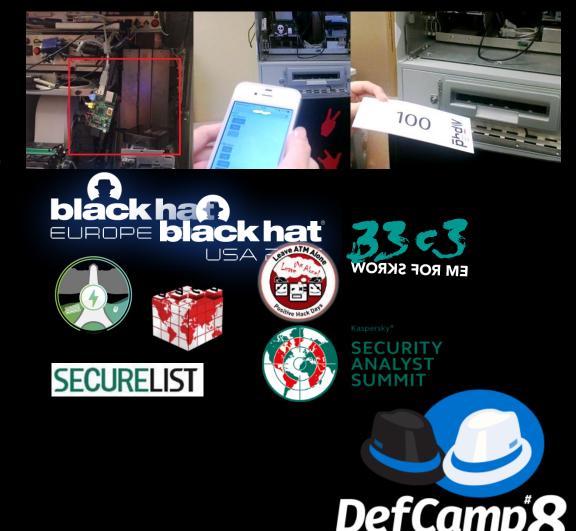


KASPERSKY

ROOT@ROOT:~# WHOAM

PENETRATION TESTING DEPARTMENT, KASPERSKY LAB

- @_ENDLESS_QUEST_, @CIFTSUNCIVEN
- ATM AND POS SECURITY ASSESSMENT
- PENETRATION TESTING
- FORENSIC INVESTIGATION SPEAKERS AT MANY IT EVENTS AUTHORS OF MULTIPLE ARTICLES, RESEARCHES AND ADVISORIES



OVERVIEW ONE SHOULD



LEGO FOR ADULTS

- TOP BOX SERVICE ZONE
 - PC
 - CARD READER
 - PIN PAD
 - OTHER
- BOTTOM SAFE
 - CASH OUT MODULE (DISPENSER)
 - · CASH IN MODULE (DEPOSIT UNIT)
 - RECYCLING MODULE (OUT AND IN)





SOFTWARE

• HOST (COMPUTER)

- OS
- GUI AND DEVICE CONTROL
- ANTIVIRUS/INTEGRITY CONTROL SOFTWARE
- VIDEO SURVEILLANCE
- RADMIN/TEAMVIEWER AND OTHER CRAP
- DEVICES
 - SOME MICROCONTROLLERS WITH RTOS



YOU CAN INSTALL KALI ON *ANYTHING* ©

@KALILINUX @DEFCAMPRO @SECESPRESSO



i 🐼 🕡 🎲 🦥 🍫 蒙

9:55 PM - 6 Nov 2017

3,115 Retweets 6,082 Likes

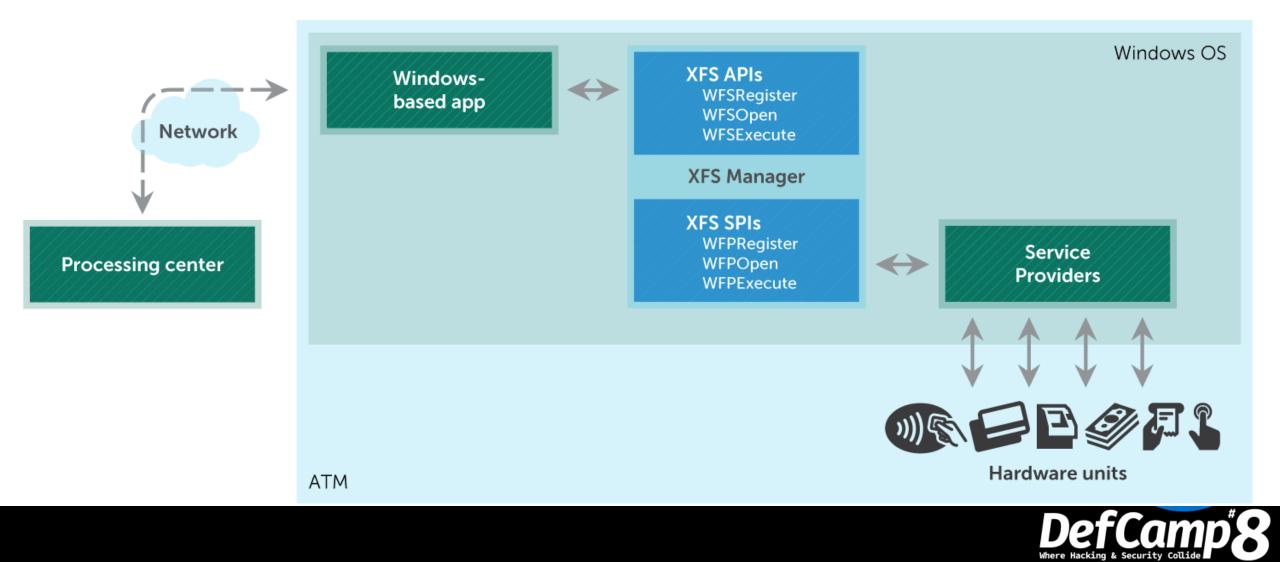


ARE YOU KIDDING ME?

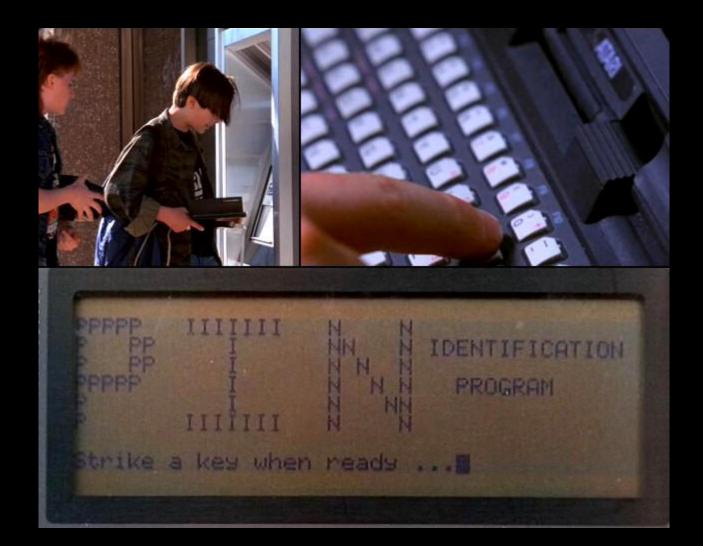




HOW IT WORKS?



THINGS FROM THE 1990S





ATTACK TECHNIQUES

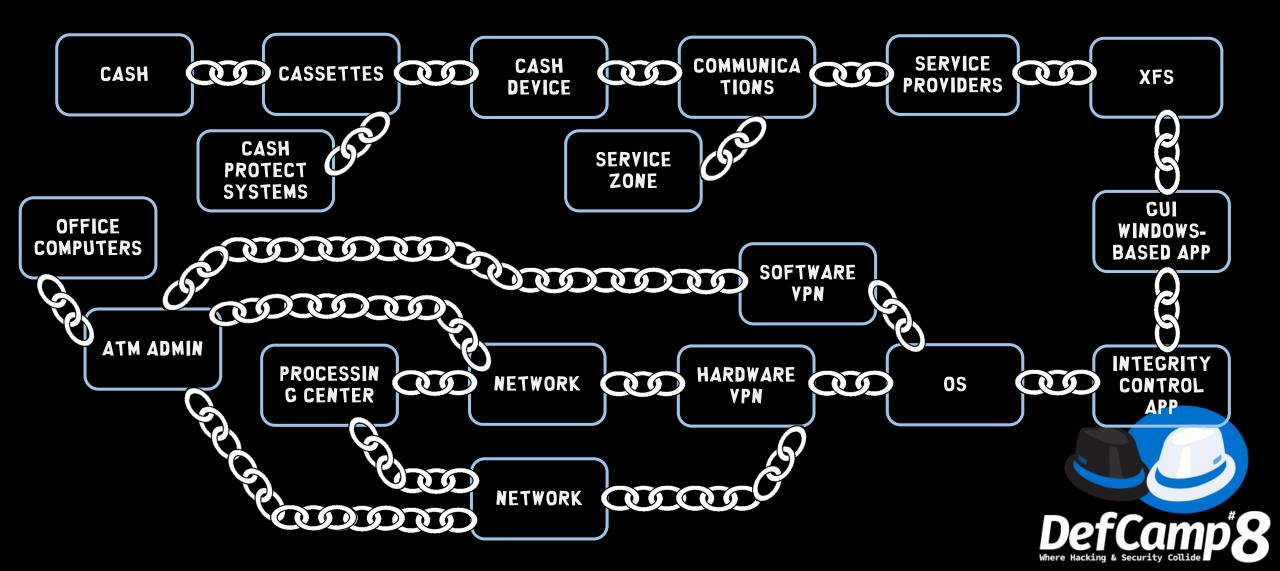
- PHYSICAL
- HARDWARE
- SOFTWARE
- NETWORK

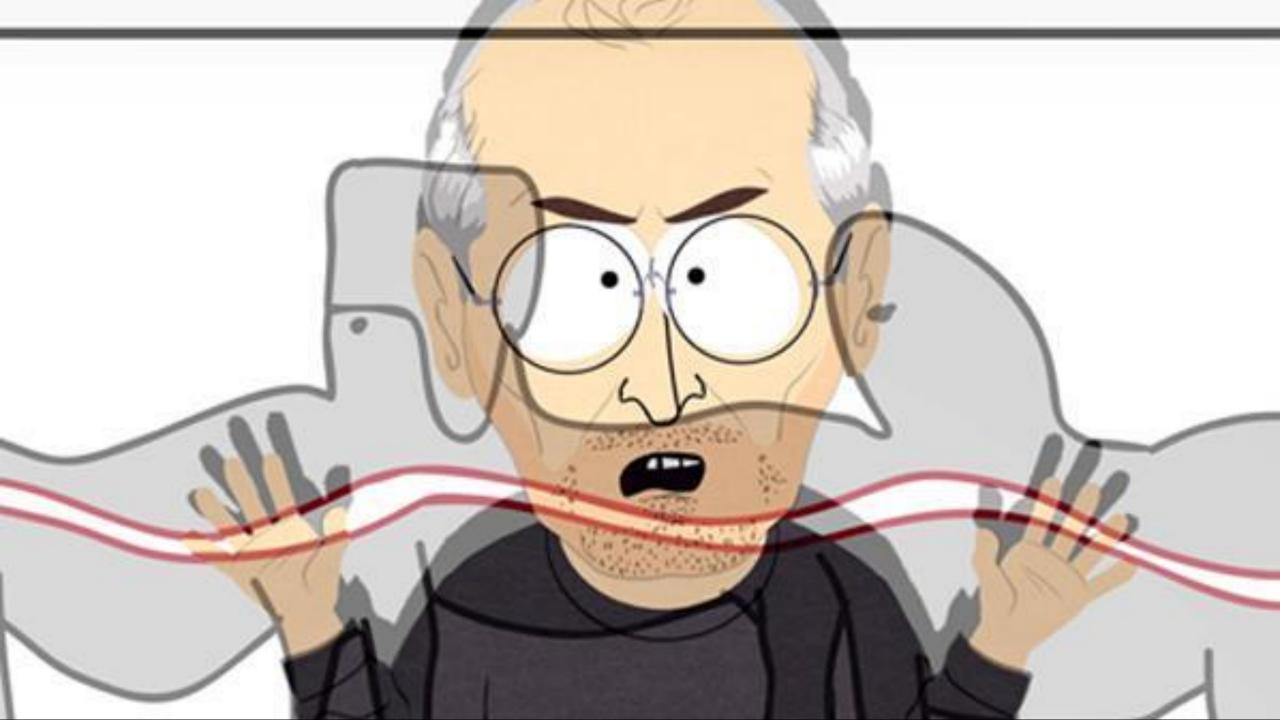


COUNTERMEASURE TO SAVE TREASURE



CASHCONTROLCENTIPEDE





CASH THEY DON'T BREAK IT. THEY STEAL.



TREASURE CHEST





DON'T BREAK THE LOCK BREAK THE CHAIN







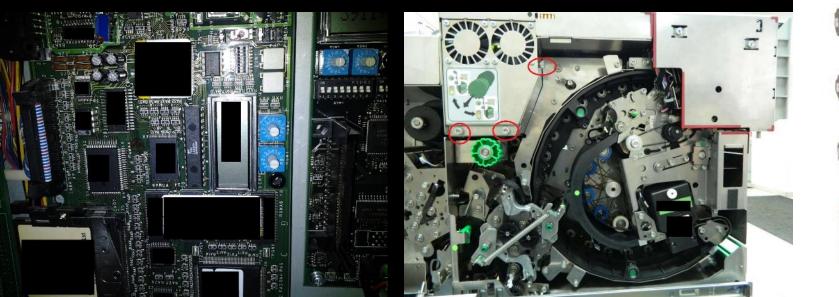


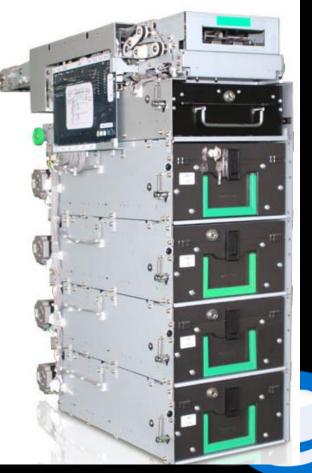
CASH DEVICES IS IN THE SAFE. SO WHAT?



WHAT IS THE HOOK

- MICROCONTROLLER
- FIRMWARE







SUPER ADVANCED PERSISTENT THREAT

- FIRMWARE
 - MODIFY
 - UPDATE
- CASH DEVICE
 - CONTROL
 - TOTAL CONTROL



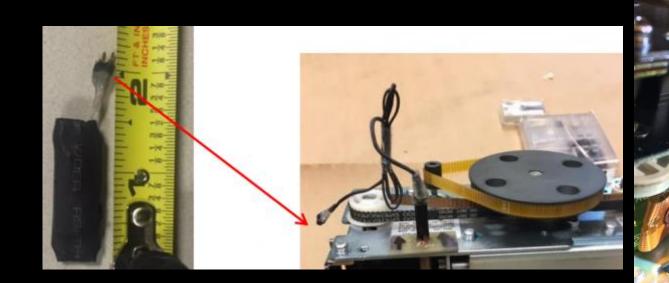
CARD READER

NOT CASH, BUT ... CASH



CARD READER EXPLOITATION

- SENSITIVE DATA IN PLAIN TEXT
- HARDWARE SNIFFER





YOU ARE NOT YOU ANYMORE

können diese Augen lügen?





SOURCE: <u>HTTPS://MEDIA.CCC.DE/Y/31C3 - 6450 - DE - SAAL 1 -</u> _201412272030 - ICH SEHE ALSO BIN ICH DU - STARBUC#VIDEO



guten Tag, mein Name ist Dr. von der Leyen







1 Ato



COMMUNICATIONS



ANALYZE THIS

- RS... (E.C. 232, 485)
- SDC
- USB



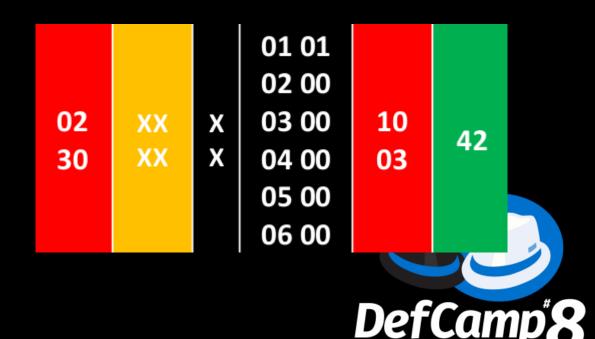
11年内第 11年内 11年の日 1	10.00 10.0	イエーハ シテス! カノノ イエーハ シテス! カノノ ・ニスイ クワハキ マスチ ・ニスイ クワロエ ヨユム ・ニスイ クフィー ・ニスイ クフィー ・ニスト スー ・ニスト スー ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	マインション シン マンション シン マンション シン モンシンション デン モンシンション マンシン マン マン マン マン マン マン マン マン マン マ	マステルマピノオ ンガ 「フォンマフノナ とヨ メーフネオスティン ソー メーフネオスティン フォ マームーン ウェキニッシーフン マームー マームー マーム マーム	チシマラノ日本ボス 900 - エテスクトボス へ本 900 - エテスクラット メ 91 - エノ 91 - エノ 9	カロオキクハウ ァキ オディレュミス オウ オデッキッテッ 0ッ コー10サンタン 10 こ つしりンタフ 10
本 3 55 本 3 55 本 3 55 本 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	インス	りりょ イノリファホン ノキトト	ステレンシン ステレン ステレン ステレン ステレン ステレン ステレン ステレン ステレ	ンコネン シスネスシウトコウスオクタ シスネスシウトファノコニク システクフロシンテンニク システクククのシンテン システレーンテンク システレーンテンシー システレーン システレーン システレーン システル システレーン システル システル システル システル システル システル システル システル	ションララノデュノロッチッ トホヨフピン トノジヌエ(トスヨフフノ シン リンジスエ(レノラコクノ コクリッレ レノラコクノ コクリッレ レノラコクノ マルク(ロク) トラスとラブスへルク	アチノ1・ホビレオオハン オクァナフオム 4モ!ヒ 0ァヱサヘ 1トコツキイ ノウヱハ ムモラソヱキ ヨウンチオユヨエクホユ
・ イン・シートン・シートン・シートン・シートン・シートン・シートン・シートン・シート	、 、 、 、 、 、 、 、 、 、 、 、 、 、	ステアスモクコチオチ ススパサエモクコチオチ ススパレスマンセルナ2: パソスンルエミクセンクリ インスンルエミクセンクリ スティクローン エンノスティクの日 エンノコクサスマイチ	し 、 し 、 し 、 し 、 し 、 し 、 し し し し し し し し し し し し し	マヘストッネ ホノリ: フオオ 1キソ デミリ: ムープクソン ビルオ・ チノホへネロ シロノ	オ 単 / コマイ/ コマ ッパ / ノンシュマ / リ ヌ オフヨウツマ ヌ ス 19二 87年 ヌ ロノオナチィッチキ ワ ロノオノ リントフ サ	■■■ 199977 13 マテ マクヌ加正 ニン
15 15 17 17 17 17 17 17 17 17 17 17	レーレーション レーン レーン レーン レーン レーン レーン レーン レー	ルラウノイオー 000 アノウノイシーオー 300 サラノマシーナ 300 サラノマシスト マク スワハシマスト 700 ローナートレート 100 セレートレート 100 セレートレート 100	レロノノカムキン (リキリニノカム マキン、フェキン いのテロンク・ノラーマ マクロンク・ノンホッ のクリフェホノンホッ 5 メシンファクス マノファファノン	ハ ノ!フハ ハ マ フレマック マ フマレスック マ フマレニュレ マ マママ マ マママ マ フママ マ ママ マ ママ マ マ ママ マ マ マ	ス アハン10オフ リ カミイェン ノ エロギルレ 上 キオムカへ マ ク チェコノラ オンノンかつラ	カーッ のノレフ ン ミワレタキ 第 ソハル集ト 5 - キ ッハキキョ 愛え
レーレーレーレーレーレーレーレーレーレーレーレーレーレーレーレーレーレーレー		キワーキワーキワー キワーキワー マンマンマスマン マンマンマスマン マンマンマスマン マンマンマスマン マン	ホホトの 国本ホト 「日本市 ション キャン レーン キャン レーン キャン レーン レーン レーン レーン レーン レーン レーン レー	772ヒクィ レオ 年オムクク ノ エトットォ ジ ラハキオム 8 ホチクパル 1 オジメ 1 ジー	ロットロット ロット	ノクギクハ コッ キャフラカ 燕ノ ユニト愛ヲ 除ハ ィキカコト クハ オホハッノ ェオ
マイレー マーレー マイレー マー マーレー マー マーレー マー マーレー マー マー マー マー マー マー マー マー マー マ		マスマス マスマス マスマス マスマス マスマス マスマス マスマス マーマ マーマ	ホイン いして いして いして いして い い い い い い い い い い い い	サンツッポコク サンクポコク サノクション マメクロ マノノのシビフ マノノの マノノマ マノノの マノノの マノノの マノノの	ア エ ス ス ス ス ス ス ス ス ス ス ス ス ス ス ス ス ス ス	フラェッホエ ヤェデォフオ オポュイェリ リフリ ハオ ヤィェ ット
マスマストレーレーン マスマストレーン マスマン マン マン マン マン マン マン マン マン マン	アノル !スッツ? 2ネス ホノーン 2マスホヲノムノン エフエホヲノムノン スコ ミヌハウノ 9ツヒロエハウィ ノフ ト21	マリンエ ソシオミ クロリフェ オシオ マルノクフ ホシオ マルノク マフオノ マオ マンオ マフオ (マンオ マンオ (マンマンノン マンノン マレ マノンノン マレ	QF オマンティンティボクト オマニテクション キャコニテクション マレクション マレクシンコン マレクシンコン マンシン マンシン マンシン マンシン マンシン マンシン マンシン	シムッピニカノマス ワムッピニカノマス ワムマチンレス サインスとキシイズ サインスとキシー レスレックスチン ストノーマチモア オノトノーマキシン オノトノーマキシン オノーキン マキン	マフノオ ク 0 ッポ カフチノフェ 4 4 4 4 カフチノフェ 4 4 4 4 メスノニ 2 つ 1 2 メノレ 5 へ 7 1 サオア マ へ 7	エスママス J コ オレスンストー 5 オヤクソンへれつ 5 トマオンスエラ / レスシュスノ J
(人) (マンマクロの) (マンマクロの) (マンマクロの) (マンマクロの) (マンマクロの) (マンマクロの) (マンマクロの) (マンマクロの) (マンマクロの) (マンマンマン (マンマンマン (マンマンマンマン (マンマンマンマン (マンマンマンマン	・ビンシテレンテレンテレンテレンテレンテレンテレンテレンテレンテレン ・アメウェンレリー ・アメウェエレリテレンテレンテレンテレンテレン ・マクラロ2015151 ・シルラレンシーンシーン・	1282 1757	・ノス二、シャッパン (スコージンタッパン (サモリンスの単一ジン (サモリンスの単一ジンス) (サージス) (サージ) (サー) (サー) (サー) (サー) (サー) (サー) (サー) (サー	************************************	・モトムヤルッッ! - ノオレッカネスス - オオレッカネスス オオピームユミ! オオマ ノハハラ エハイ マネへ? エノカノ マカク・	・イデョイを マテクペンション マテクペンション マテノフンエラ マースストン シンロ第11 シンロ第11 シンロ第11
		マクレロ ス マクト ス マクト ス マクト ス マクト ス マクト ス マクト ス マクト ス マース ス マース ス マース ス マース ス マース ス マース ス マース マー	ハウハァの サウハァの シノラ 4 1 シリノラ 4 1 シリノラ 4 2 チリノク 15 チセワ 7 チセワ 9	スレノノリシ シロマノサシ シロマメマクク リウネラクク リウキソカ シスカハロ シクトハロ シク ノ	83 ホピロス マシストン マシストレン シシストレン シシストレ マシン マシン マシン マシン マシン マシン マシン マシン マシン マシン	オルロフ 9 ツ 8ネジ ソニルヨ
イントレート ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	、 0 マン 1 0 マン 1 0 マン 1 1 1 1 1 1 1 1 1 1 1 1 1	1000000000000000000000000000000000000	キマス ママスマン ママスマン マステノス マステノス ママン ス マス レ ママン ノ ス ママン ママン ママン ママン ママン ママン ママン ママン ママン マ	トーママス トーマ トーマ トーマ トーマ トーマ トーマ トーマ トーマ	フェノノロン サイフロマ モリアフィー リノモカマハー して手ビノデフ レーマル レーオ	うキンホウ ィツノウノ ッユクロック フニサフヤノ
ホレス 本 し 本 た て 、 ホ て 、 、 、 、 、 、 、 、 、 、 、 、 、	キ フロロンニレトッ4 スクムンニロのロノマ マチノカマミスノ マラミノマ	ファノミュア ロサキトマワ マサキトマワ マチフピピ マチマ マチマ マチマ マ マ マ マ マ マ マ マ マ マ マ マ マ	オワノカンソート キャーション オフタノタリン クリス フルミス レーション マック フルミス ステ マック マック マック マック マック マック マック マック ファノカン マック マック マック ファノカン マック マック マック マック マック マック マック マック マック マック	マノェス マンコオ キンション サリー マー マー マー マー マー マー マー マー マー マー マー マー マー	ジャマノノノメ シレーマニマッ ■ノソノフノッ ■ノソノフノッ	ノ 101年 キ ノメマ ち フスフ キ ホノ 2



TYPICAL FLAVOURS



- ASCII-BASED
- BINARY
- ENCRYPTED OBFUSCATED



HACKER STUFF









VIDEO - NEWLY EVIL USB (BLACKBOX)



HTTPS://YOUTU.BE/3HYAOMVIZPM

SERVICE ZONE

THERE IS NO CASH. REALLY?



HOW TO GET IN

- "MASTER KEY"
- SCREWDRIVER

Buy Now

• "SPECIAL" TOOL



Buy Now

S.



Alexander Zaitsev

@arbitrarvcode



Who buys these ATM keys? Tell locksmith the code and get it cut. Totally unrelated: why is it "Top selling product"?

D Followi

Item condition: Quantity:

Best Offe





VIDEO - HOW TO GET IN

HTTPS://YOUTU.BE/KIJIZHUTLJU



OUR SERVICE ZONE IS SECURED ©





SHOULD WE?



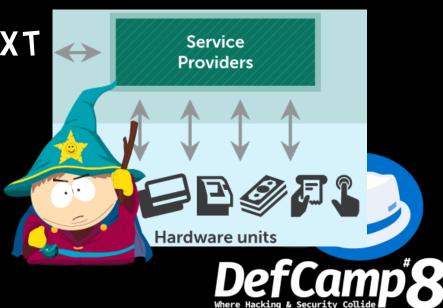


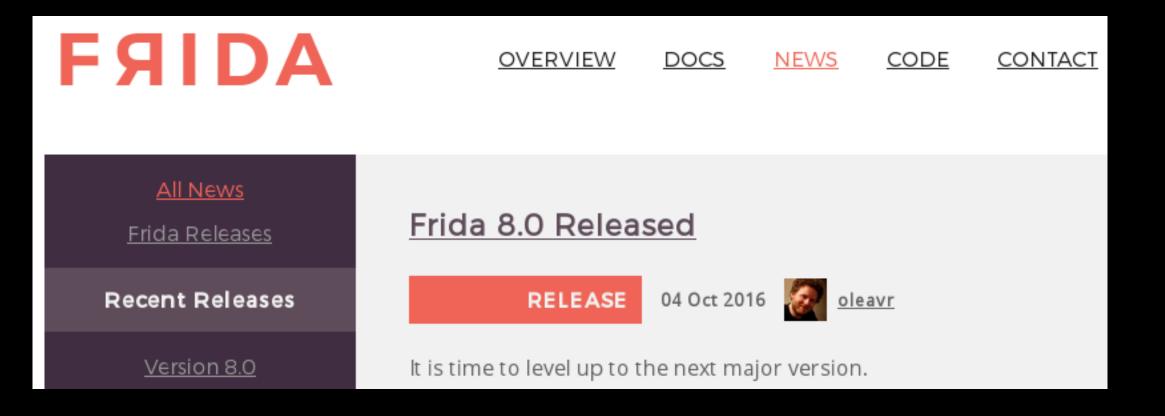
SERVICE PROVIDERS



MALWARE: NEXT GENERATION

- ATTACKER BYPASSES INTERACTION WITH XFS MANAGER
- HOOKS ALL FUNCTIONS USED BY SPECIFIC ATM VENDOR SOFTWARE
- GIVES HIGHEST INFORMATION TO ATTACKER COMPARED TO XFS BASED MALWARE:
 - INTERCEPT NETWORK DATA IN CLEAR TEXT
 - INTERCEPT EMV TRANSACTIONS
 - INTERCEPT USB/COM COMMUNICATION





Quick-start Instructions

~ \$ sudo pip install frida ~ \$ frida-trace -i "*dispens*" service_provider



VIDEO – MALWARE NG

HTTPS://YOUTU.BE/XOKG7HNVT20



MALWARE: XFS BASED

- EVERY WINDOWS EXECUTED CAN ISSUE COMMANDS TO XFS MANAGER
- MALWARE CAN WORK ON MOST ATMS
- EVERYONE INVOLVED IN ATM SECURITY IS PRETTY MUCH FAMILIAR WITH IT



DEVOPSSECHUMANCATERPILLAR

- BUFFER OVERFLOW
- KIOSK MODE BYPASS
- SENSITIVE DATA DISCLOSURE





THIRD-PARTY SECURITY SOFTWARE ONE MORE DOOR

- BUFFER OVERFLOW
- KIOSK MODE BYPASS
- SENSITIVE DATA DISCLOSURE
- REMOTE CONTROL





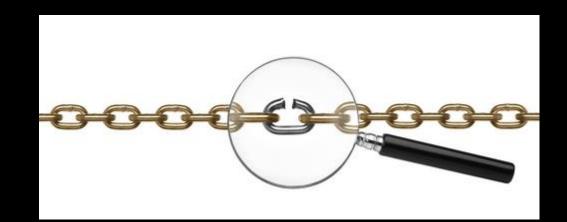
OPERATING SYSTEM

MS08-067 STRIKES AGAIN

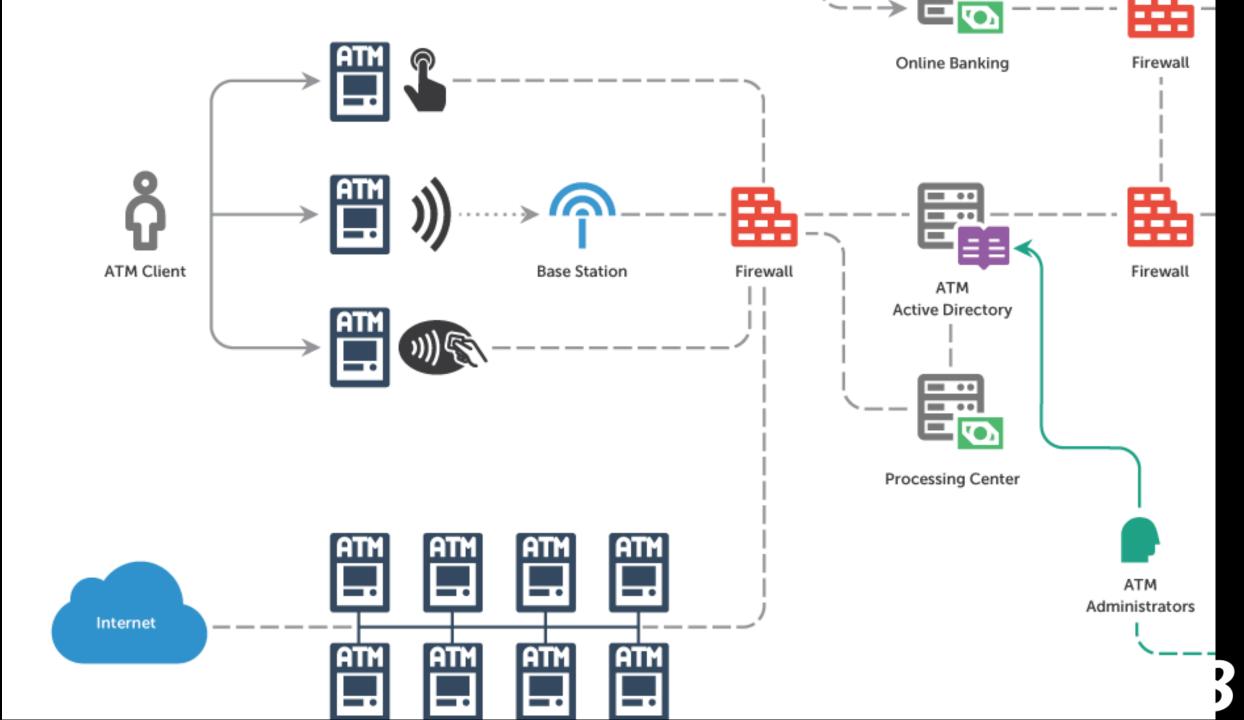


JUST AHEAD

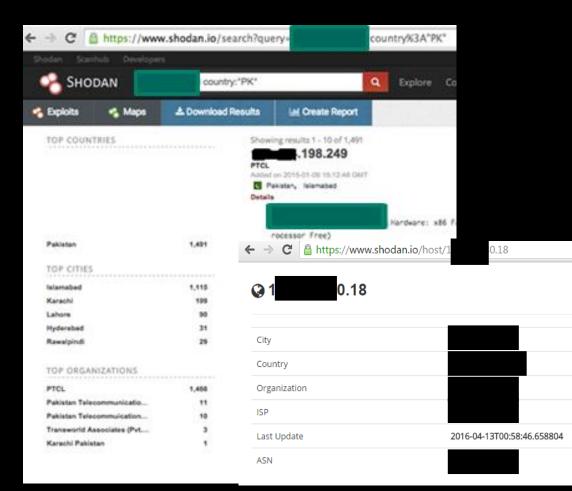
- OLD VERSIONS
- NOT UPDATED
- VULNERABILITIES
- STANDARD SERVICES







LET'S HAVE FUN WITH SHODAN



10 mil 10 mil			
37	NetBIOS Response		
udp	Servername: ATM		
etbios	MAC: : :f7:cf:bf		
	Names:		
	ATM <0x0>		
	WORKGROUP <0x0>		
	ATM <0x20>		
	WORKGROUP <0x1e>		
	WORKGROUP <0x1d>		
	MSBROWSE <0x1>		
		amily 6 Model 22 Stepping 1 1d 2600 <mark>Multiprocessor Free</mark>	
udp snmp		ld 2600 Multiprocessor Free	
dp mp are: Win 45 cp	dows 2000 Version 5.1 (Bui Anonymous login success	ld 2600 ^M ultiprocessor Free ful	
ip mp are: Win 45 p	dows 2000 Version 5.1 (Bui Anonymous login success Sharename	1d 2600 Multiprocessor Free ful Type Comment	
udp nmp ware: Win 445 tcp	dows 2000 Version 5.1 (Bui Anonymous login success Sharename	1d 2600 Multiprocessor Free ful Type Comment	.)
dp mp are: Win 45 Cp	dows 2000 Version 5.1 (Bui Anonymous login success Sharename Error returning browse	ful Type Comment List: NT_STATUS_ACCESS_DENI	.)
udp nmp ware: Win 445 tcp	dows 2000 Version 5.1 (Bui Anonymous login success Sharename	ful Type Comment List: NT_STATUS_ACCESS_DENI	.)
udp mmp ware: Win 445 tcp	dows 2000 Version 5.1 (Bui Anonymous login success Sharename Error returning browse	ful Type Comment List: NT_STATUS_ACCESS_DENI	.)
udp snmp tware: Wit 445 tcp	dows 2000 Version 5.1 (Bui Anonymous login success Sharename Error returning browse Anonymous login success	1d 2600 Multiprocessor Free ful Type Comment 	.)
idp hmp ware: Win 145 top	dows 2000 Version 5.1 (Bui Anonymous login success Sharename Error returning browse Anonymous login success	1d 2600 Multiprocessor Free ful Type Comment List: NT_STATUS_ACCESS_DENI ful Comment	.)
udp nmp ware: Win 445 tcp	dows 2000 Version 5.1 (Bui Anonymous login success Sharename Error returning browse Anonymous login success Server	1d 2600 Multiprocessor Free ful Type Comment List: NT_STATUS_ACCESS_DENI ful Comment	.)
udp snmp tware: Win 445	dows 2000 Version 5.1 (Bui Anonymous login success Sharename Error returning browse Anonymous login success Server ATM	1d 2600 Multiprocessor Free ful Type Comment 	.)

112

Where Hacking & Security Collide

VIDEO – OBEY THE NET

Def Camp # 8 Where Hacking & Security Collide

HTTPS://YOUTU.BE/N9DJTYO-COO

WHY VPN IS NOT GOOD SOMETIMES





• SOFTWARE

- WITH ACCESS TO OS CAN BE DISABLED
- NOT ALWAYS PROVIDE FIREWALLING FUNCTIONALITY
- IF VPN-CONNECTION IS INTERRUPTED IT IS COMMON, THAT ALL DATA FROM THIS MOMENT WILL BE TRANSMITTED IN CLEAR-TEXT
- HARDWARE
 - DOESN'T PROTECT AGAINST PHYSICAL ACCESS
 - WORKS REGARDLESS OF HOST COMPUTER
 - IT'S PEACE OF METAL/PLASTIC, YOU CAN GRAB IT WITH HAND



PROCESSING CENTER



TWO-EDGED SWORD

- ROGUE PROCESSING CENTER (ATTACKING ATM)
 CASH WITHDRAWAL
- ROGUE ATM (ATTACKING PROCESSING CENTER)
 - FAKE CASH DEPOSIT
 - BANK CARD ACCOUNT COMPROMISE
 - PAYMENT SERVICES/SYSTEMS ATTACKS



VIDEO – ROGUE PROCESSING



HTTPS://YOUTU.BE/NRBQBLBLLLS

НОЖ ТО



WHAT TO BREACH

- COALS
 - SENSITIVE DATA DISCLOSURE
 - UNAUTHORIZED CASH WITHDRAWAL
- WAYS
 - NETWORK
 - COMMUNICATIONS LINES
- POINTS
 - BASED ON THE COMPLEXITY OF THE FINDINGS
 - ATTACKS OVER USB BRING YOU EXTRA POINTS



RULES

- READ FULL VERSION HERE <u>HTTPS://DEF.CAMP/HACK-THE-</u> <u>BANK/</u>
- HACK THE BANK CAREFULLY DISRESPECTING ANY OF THESE RULES AS WELL AS ANY OFFENSIVE ACTION TAKEN AGAINST ANY OTHER PARTICIPANTS WILL RESULT IN IMMEDIATE DISQUALIFICATION
- P.S. MODERATORS ARE ALWAYS RIGHT ^_^



KASPERSKY

HAVE FUN Stay safe

OLGA KOCHETOVA, OLGA.KOCHETOVA@KASPERSKY.COM, @_ENDLESS_QUEST_

ALEXEY OSIPOV, ALEXEY.OSIPOV@KASPERSKY.COM, @GIFTSUNGIVEN

