

# Physical Theft Meets Cybercrime: The Illicit Business of Selling Stolen Apple Devices

**Technical Brief** 

TrendLabs Security Intelligence Blog Fernando Mercês and Mayra Rosario Fuentes Forward-Looking Threat Research (FTR) Team November 2017

# **Table of Contents**

The Modus Operandi	1
AppleKit: iCloud Fraud as a Service	5
MagicApp: Automating iCloud Fraud	7
iUnlocker: MagicApp's Affiliate	0
Cybercriminal Collaboration: How the Fraudsters Run their Business	3
Physical and cyber security go hand in hand	17
Indicators of Compromise (IoCs)	8

#### TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

It's not difficult to imagine why there'd be a large, global market for stolen mobile phones. From <u>Ireland</u> and <u>the U.K.</u> to <u>India</u>, <u>Argentina</u>, and <u>the U.S.</u>, the demand for unlocking services for stolen phones is staggering: last year, stolen iPhones were sold in Eastern European countries for as much as US\$2,100. Online marketplaces like eBay and Mercado Libre also sell iCloud-locked phones—usually stolen or lost—although they're sometimes advertised as "sold for parts" to avoid having the listing removed.

Conversely, we've found that it also goes beyond physical theft. This was illustrated by an <u>incident</u> we delved into last May, where an iPhone theft intersected with cybercrime. Further scrutiny into this unique crossover revealed how common it is as a business.

Our research led us to certain tools that their developers and fellow fraudsters use to unlock stolen or lost Apple devices: AppleKit and MagicApp, as well as a cybercriminal version of the Find My iPhone API, along with phishing kits and other related services. These tools entail hijacking iCloud accounts and certain Apple services tied to the device then reactivating them in order to resell the devices on various marketplaces.

	Apple iPhone 6 A1549 VERI Pre-Owned - iPhone 6 - 16GB - Ver	ZON Silver Space Gray LOCKED READ DESCRIPTION	0.0	
	\$74.00 Buy It Now Free Shipping View similar active items Sell one like this	Sep-27 16:57	*	Here
	APPLE IPHONE 6 PLUS Spr Parts Only - IPhone 6 Plus	ace Grey A1524 **Locked* READ DESCRIPTION**!!		
an Marian Marian Marian Marian	\$50.00 Buy It Now +\$4.36 shipping	Sep-27 13:05	\$ 2,850	\$ 2,800
	View similar active items Sell one like this		12x \$ 281~ Iphone 6s 16gb Perfecto En Estética, Con Bloqueo De Icloud	Iphone 6 Bloqueo Icloud

Figure 1: Ads from eBay (left) and Mercado Libre (in Mexican pesos, right) for iCloud-locked iPhones

## The Modus Operandi

Apple's iCloud isn't just a cloud storage service. If iCloud is linked to an Apple ID, the device's owner can lock the phone (via Apple's Find My iPhone settings) if it gets lost or stolen, requiring a password to reactivate the phone and its features.

<u>Erasing</u> the device and disabling the Find My iPhone service used to be all it took to unlock a lost or stolen device. iOS has since added anti-theft tools that prevent stolen or lost phones from being reused, such as Activation Lock (added to iOS 7 in 2013) and <u>Find My iPhone</u>. The latter can track the device using GPS and displays the device's approximate location on a map in real time. Only the device's owner can turn the feature on or off. Without the owner's Apple ID and password, lost or stolen phones cannot be erased or reactivated for another user.

Activation Lock works by using the iPhone's International Mobile Equipment Identity (IMEI) or serial number to check if the iCloud Activation Lock is disabled. However, Apple stopped the "activation lock checker" website that verifies Activation Lock in January 2017. An instructional video posted on YouTube showed how to misuse Activation Lock to discover valid IMEI. By exploiting a vulnerability, it can be abused to trick Apple's servers into unlocking a non-functional iPhone or iPad.

Below is a visualization of the modus operandi, exemplified by a real-life victim we interviewed and worked with after his iPhone was stolen on the streets of Brazil. Shortly after activating Apple's Find My iPhone, he received a phishing SMS on his new phone (which retained his old number) that redirected him to a legitimate-looking webpage asking for his Apple ID. Fortunately, he saw through the scam, and his login information didn't fall into cybercriminal hands. If phished successfully, the scammers could've made off with his credentials, which can be used to take over his Apple ID to unlock his stolen iPhone and delete the accounts linked to it.



Figure 2: Phishing attack chain to unlock iCloud accounts

Once attackers have hijacked the victim's iCloud, their tools also enable them to download the iCloud account (to perform other malicious activities) and then delete it.

We found parts of the source code of one of the phishing pages in an open Github repository that also kept different tools for building iCloud phishing pages. The phishing page is based on what cybercriminals call *FMI.php*, (Find My iPhone) / Devjo class, a component present in many other phishing kits. It's the closest tool cybercriminals have that resembles the Application Program Interface (API) of Apple's own Find My iPhone.

<b>C</b> Fea	tures Business Explore	Marketplace	Pricing	This repository S		Sign in or Sign up
-	/ icloud				♥ Watch 0	Star 0 % Fork 0
<> Code	() Issues 0 11 Pull requ	iests 0 🔢 Proj	jects 0 Insi	ights <del>-</del>		
Branch: mas	icloud / FMI.php					Find file Copy path
	Add files via upload					0b45147 on Mar 21
1 contributo	r					
104 lines (	95 sloc) 3.37 KB				Raw Blame	History
2 //D 3 cla 4 5 pri 6 'Or 7 'Us 8 'Cc 9 'Ac 10 'Re 11 'Ac 12 'Ac 13 ); 14 pri 15 pri 15 pri 15 pri 20 21 22	<pre>ont change any thing in this f: ss Devjo { vate \$headers = array( igin: https://www.icloud.com ', rerAgent: Mozilla/5.0 (Windows ntent-Type: text/plain ', cept: */*', ferer: https://www.icloud.com/ cept-Encoding: gzip, deflate ', cept-Language: en-US,en;q=0.8 vate \$username; vate \$username; vate \$username; vate \$username; vate \$username; vate \$username; vate \$username = \$user; \$this-&gt;username = \$user; \$this-&gt;user</pre>	<pre>ile :Dyes api YOU C#</pre>	N CHANGE THE nar leWebKit/537.36 ( login";	me here (KHTML, like Gecko) Ch is->password.∵","exten	rome/45.0.2454.101 Safar: ded login":false}';	1/537.36 ' <i>,</i>

Figure 3: A fake Apple verifier phishing script project on Github (March 21, 2017)

Once users enter their credentials into the phishing page, the FMI.php framework API is used to retrieve the user's iCloud information, log in to the iCloud website, and receive Apple device information. We tested the phishing page and received information such as cell phone number, passcode length, ID, GPS location, whether the device is locked or not, and if there's a wipe command in progress. FMI.php framework can also delete the device from the victim's Apple account after it's unlocked and notify the attackers by email once the victim has been successfully phished, as shown in Figure 4. "True Login" means the FMI.php framework backend-tested and verified the validity of the iCloud credentials. The phishing kits are available in English, French, Spanish, and German.



Figure 4: The information that FMI.php API collects from iCloud



Figure: 6: Screenshot of languages (left) available for the phishing page (right)



Figure 7: Screenshot of a YouTube Video on how to use an iCloud phishing kit

### AppleKit: iCloud Fraud as a Service

AppleKit is not limited to iPhones; it also supports iPad, Mac, and Apple Watch models. The unlocking service is also available to those without any technical know-how—they need only pay an upfront fee to unlock the devices within hours or days. The website dakarunlock[.]com, for instance, has a price list of unlocking services depending on the carrier and country. The seller uses AppleKit and another software called MagicApp to run his unlocking business. AppleKit was sold for \$500 prior to September 2017 but is now offered for \$300.

••• <> D		& & © 0	-	-	c	0 0
- Catch up tools 😫 kit		How Many Victim's	Mail Sent		How Many IOS	How Mar
삼 Victims	e	9 Victim's	🖌 80 eMail's	L.	2 Device's	<b></b> 2 Devi
&x Failed attempts	1			1		
- Sender 🛍 kit						
🖾 Email	( <b>.</b>		Apple <b>s</b> kit Simp	le But Powe	ərful	
🗭 Sms	¢		The Most Advanced And Powerful- T	he Most Effective Ar	nd Powerful Way.	
Template	e.					
î Cron Jobs	۴	Check FMI by IMEI				
API	: <b>16</b> 5				5	- 14
- Tracks Tools					5	Tel .
Track Sys	5					
A Visitor	۲.	<ul> <li>Visitor Online</li> </ul>				
Block/Banned	¢	It will display the last visitor online automatically refresh #  ♀ IP  ♀ is Mobile  ♀ ii	every 5 min. s Bot ? ≎ Last Seen ≎		Last Place Visited \$	٠
Admins	<	+1 📵 => 🌉 No N	lop a Human Thu, 28 Sep 2017	- 05:08 pm	I will be a series	· Bioch
GIE				· 1 · =		

#### Figure 8: AppleKit's control panel

#### iCloud Remove And Apple ID Service

Service Name	Туре	Delivery Time	Price
Apple ID Find Service iPhone/iPad By IMEI AT&T (Name+Number) [100% Info]		1-3 days	USD25USD
Apple ID Find Service iPhone/iPad By IMEI Sprint (Name+Number) [100% Info]		1-3 days	USD32USD
Apple ID Find Service iPhone/iPad By IMEI T-Mobile (Name+Number) [100% Info]		1-3 days	USD20USD
Apple ID Find Service iPhone/iPad By IMEI Verizon (Name+Number) [100% Info]		1-3 days	USD25USD

Figure 9: Price list for unlocking Apple devices located in the United States (from dakarunlock[.]com)

IMEI Service			
ICLOUD TOOLS	Price	Туре	Delivery Time
REMOVE FIND MY IPHONE LOCK (ICLOUD) - USING OWNER EMAIL/MOBILE - CLEAN & LOST	\$60USD	8	1-15 Days
REMOVE FIND MY IPHONE/IPAD LOCK (ICLOUD) - APCOM/ORANGE/VODAFONE ROMANIA - LOST	\$110USD	-	4-20 Days
REMOVE FIND MY IPHONE/IPAD LOCK (ICLOUD) - APCOM/ORANGE/VODAFONE ROMANIA - CLEAN	\$80USD	-	4-20 Days
REMOVE FIND MY IPHONE LOCK (ICLOUD) - LIMITED COUNTRIES - CLEAN	\$145USD	-	5-35 Days
REMOVE FIND MY IPHONE/IPAD LOCK (ICLOUD) PURCHASED IN RUSSIA - CLEAN	\$65USD	-	1-14 Days
REMOVE FIND MY IPHONE/IPAD LOCK (ICLOUD) PURCHASED IN IRELAND - CLEAN	\$180USD	-	4-20 Days
REMOVE FIND MY IPHONE/IPAD LOCK (ICLOUD) PURCHASED IN UNITED KINGDOM - CLEAN	\$105USD	9	5-25 Days
REMOVE FIND MY IPHONE 7/7+ LOCK (ICLOUD) - SOLD BY APPLE STORE USA/CANADA- CLEAN	\$235USD	-	3-20 Days
REMOVE FIND MY IPHONE 6S/6S+/IPAD PRO LOCK (ICLOUD) - SOLD BY APPLE STORE USA/CANADA- CLEAN	\$210USD	-	3-20 Days
REMOVE FIND MY IPHONE 5/5S/SE/6/6+/IPAD LOCK (ICLOUD) - SOLD BY APPLE STORE USA/CANADA- CLEAN	\$170USD	-	3-20 Days

Figure 10: Price list of iCloud-unlocking services (from i-IMEA)

## MagicApp: Automating iCloud Fraud

MagicApp automates the unlocking of iPhones and used in conjunction with other attack vectors. The app has a list of supported devices, via Universally Unique Identifier (UUID). MagicApp can also run on jailbroken Apple devices, as it is not approved on Apple's official App Store. MagicApp's website, iosdev[.]asia[:]2403, is designed to appear legitimate, what with its use of Apple logos.

As of October 1, MagicApp is offered for free, with several links provided on its website. To complete the unlocking process, however, one has to work with other purveyors who will provide phishing and text messaging services. They are paid per unlocked device. MagicApp's source code is also on Github. The app has specific developer/team names and UUIDs for devices to run, as seen in Figure 11.

lome >	Sample In	formation					
Basic	info plist	file map	main macho	other macho	itunes meta data plist	embedded mobile provision	
							vie
Creati	onDate		2017-04-23 2	20:02:34			
Name							
AppID	Name		MagicApp Tv	<b>/</b> 0			
Applic	ationIder	ntifier <b>P</b> re	fix				
Platfo	rm		iOS				
Versio	n		1				
TimeT	oLive		364				
Team	Name		The second second				
Teaml	dentifier		10.000				
Develo	operCerti	ficates		5.50		071020-00	

Figure 11: Snapshot of MagicApp's properties on Github



Figure 12: Snapshot of MagicApp from its website

MagicApp offers a full range of features for unlocking stolen devices. Among them is the capability to send phishing emails or text—pretending to be from Apple—designed to steal the victim's iCloud credentials. Every field is customizable, enabling bad guys to send texts in their local language. It can also send a fake GPS location to deceive the victim into believing their lost phone was found.



Figure 13: MagicApp's templates for phishing messages are easily editable



MagicApp offers 50 customizable phishing templates for each Apple device. Of note is the attention to detail (i.e., fonts, spacing, box elements, and colors). The idea is to phish a victim with a message that's identical to the real email Apple sends when a lost device is found. MagicApp supports iPad Air, iPad Air 2, iPad Mini, iPad Pro, iPhone (4S, 5, 5S, 6, 6S, 6+, 7, 7+), and Apple Watch (series 1, 2).

#### iUnlocker: MagicApp's Affiliate

iUnlocker supports various countries and their respective carriers. Price varies depending on the carrier and country; the estimated time for the services also differs, which we suspect may be a manual process that involves colluding with other fraudsters. Clearing an IMEI with iUnlocker is also priced differently. The same service will cost \$9.99 for AT&T phones, \$117.99 for T-Mobile, and \$66.99 for Bell Canada phones.



Figure 14: Code snippet using iUnlocker to check the device's IMEI (analysis by Ju Zhu)



Figure 15: iUnlocker's list of supported carriers



Figure 16: iUnlocker's price for the same service for different carriers

MagicApp's developer offers other services like phishing as a service, either via SMS or email, to unlock iCloud accounts if the customer does not have a server set up (or is unwilling to pay for one). These services purportedly guarantee that the phishing messages will actually arrive and not identified as spam.



Figure 17: An advertisement on Twitter offering iCloud spam services using MagicApp

#### Cybercriminal Collaboration: How the Fraudsters Run their Business

The schemes we uncovered involve several fraudsters from Kosovo, Philippines, India, and those in North Africa. We monitored three notable actors who often worked together, and whose products and services are commonly used together: Mustapha\_OS, Engine\_App, and i\_phisher.

Mustapha\_OS is AppleKit's developer, and is also known to participate on dev-point, <u>an Arabic hacker</u> <u>forum</u>, as early as 2008. Engine\_App developed MagicApp, while i\_phisher provides phishing scripts and sells server services for SMS messaging. Customers using MagicApp or AppleKit aren't obligated to use i\_phisher's phishing scripts, but because they know each other's products well (and have a high success rate), many tend to use all three. Customer satisfaction can be seen on Twitter, which includes screenshots of the devices they've unlocked. The three can also be reached through the notably <u>misused</u> application, <u>Telegram</u>.



Figure 18: A Tweet of a satisfied MagicApp customer showing the unlocked iCloud device.



Figure 19: Mustapha\_OS's post on dev-point discussing his experience of installing MacOS on his Dell Inspiron Windows computer

Mustapha\_OS used to be active on Facebook but now appears to be using his Twitter account daily. For his latest version of AppleKit (September 2017), he worked with a fellow fraudster going by the moniker DiamantOsmani on Twitter to fine-tune the features of Find My iPhone API. DiamantOsmani has been in the unlocking business for at least five years, according to his online hacker profiles and forum activities. He has also posted various instructional videos on how unlocking iPhones work via social media. Support for AppleKit is provided by another who goes by the handle icloudtruth1.

Engine\_App and i\_phisher occasionally team up to offer customers special pricing for using their tools together. i\_phisher once posted pictures of logo designs, and we saw one that Engine\_App previously used. i\_phisher also used the monikers icloudphisher and cloudphishers on social media accounts, and runs his own device-unlocking business (i[-]unlocker[.]com).



Figure 20: i\_phisher requesting to exchange different currencies

i\_phisher also offers other services: logo designs as well as fake Apple Store and telecom carrier receipts. The receipts are for people requesting Apple (via Apple's stores or online chat) to unlock the iCloud-locked device, as Apple's policies require the device's owner to show an invoice or receipt as proof of purchase. It's not known if this technique always works or if these fake receipts are actually verified.

the second se	en managemente a -en as some
	INVESTIGATION CONTRACTOR OF A DESCRIPTION OF A DESCRIPTIO
and the second	1994
	Formation the second in the se
	4140 46,12,4040 (1997)15 75,115 8,46 8,46
	Inter La de
	electronic an test forces and test an electronic and the second
- tot	and the second and and a second and and a second and and a second and a second and a second and a second and a
atel	
acas	
OTODE	
RETAIL STORE	
and the second s	REPORT OF A DESCRIPTION OF
A CONTRACTOR OF	
	ENTERTAINMENT-ELECTRONICS
	IPAD MINI WIFI 16GB \$399.00
NO. 8	#P#File= - : )3
STORE NO. REGISTER NO.	
	SUBTOTAL \$399.00
1	YOUR REDCARD SAVINGS 5% \$19.00-
	TOTAL \$404.34
CUSTOMER	*6289 TARGET VISA \$404.34
SALE C MM FACE GRAY 649.99	INDICATES SAVINGS
IPHUNE 6 HH 0460 CHILL CAR	
SER.NU.	
IMEI:	
	and the second se
SIM 0.00	
SER.NO.	1111
	and a second sec
	and a state of the
SUBTOTAL 649.99	
TAX 40.86	
TOTAL AMOUNT DUE 690.85	
DEBIT CARD TENDERED 500 PE	12 A.
	and and a second

Figure 21: Sample fake Apple Store and telecom carrier receipt for an iPhone 6 customer in the U.S.

mil arouan ×	Twente Followine Followers Likes Lists ★ M AppleCare Cas ≠: 10693: ★	
← ⇒ C		
Google	۹	
Gmail +	←	
COMPO SE	AppleCare Case #:	÷ 2
Inbox (333) Starred	to me 💌	12:17 PM (8 hours ago) 📩 🔸 🝷
Important	н	
Sent Mail Drafts (3)	I just checked your records and we have yet to receive information from the validation team. Their response general may have to wait until Wednesday for an update. I hope this helps.	ly takes about 4 working days so we
- Categories	Have a good evening	
2 Social (698)	Best regards,	
<ul><li>Promotions (426)</li><li>Updates (310)</li></ul>	AppleCare Senior Advisor AppleCare - Asia-Pacific	
10 (1)		
Constant of the local division of the local	On 21 Mar 2016, at 7:04 PM,	

Figure 22: i\_phisher showing his interaction with AppleCare via his Gmail account

#### Physical and cyber security go hand in hand

Just as the internet has evolved the way <u>information</u> is accessed and shared, or how businesses are conducted, it has also blurred the face of crime. It's no longer confined to the brick-and-mortar theft. The online tools we've seen show how traditional felony and cybercrime can work concertedly—or even strengthen each other—for bigger payouts. Last September, for instance, cybercriminals got hold of iCloud credentials and abused Apple's Find My service to <u>lock</u> Mac users out of their device then extort them. The potential impact: resetting the device and losing all its data.

Ultimately, physically securing devices shouldn't take a back seat. But apart from keeping an eye on your devices, awareness also plays a crucial role. Apply <u>best practices</u> for <u>securing mobile devices</u>, especially those that use <u>Bring Your Own Device</u> programs. <u>Regularly back up</u> data stored on them, and be more prudent against <u>phishing</u>.

More importantly, do your research: if purchasing a secondhand device, verify with the vendor or carrier that they're not blacklisted. The Cellular Telecommunications Industry Association (CTIA) created a <u>website</u> that verifies the IMEI to help customers and law enforcement check if an iPhone has been blacklisted or stolen. Resellers and consumers alike should also note that historical data from the device's Find My iPhone is saved on Apple's databases. Smartly enough, Apple devices have preventive measures in place that make stealing and reselling devices tricky, including one that can brick a stolen device.

# Indicators of Compromise (IoCs)

#### Hashes related to the phishing kits (SHA-256):

Hashes	Trend Micro Detection
1b02900b3f5ad19e526475b626134e3debe4a3fe5178fd2c3dd30c9a256c9b82	
848de54914d1da0ee9a8b99f97b71ac37decf1359dc378d28310a60705ca69c6	PHP_PHISH.IJ
142918c2370e27c83560de0345612d5f75b24306b2c513d130ee10d48950416a	
3d60e153fc34ec0cb5437f3e8e9867175ceca16f1b24d1fd5c8f206b3a8e54b3	
4ad7b1f5f32a9dc81cc5adbfba667fb09e80358a64762816801aff731c545757	
7f40752e5ec2d64458d92b88a115cc1018acface5a800b71a933999ec141e280	
014a2af6b0552a4b8fa4f9c7b4239e6a73542d2c77d717c7812dca95522d6176	
b999f27b14eac83bbba5cbe772fa437c138de21477fba6c82fc65a4f55a30626	
d8211cd5b1227e202471d26644537b19904b93b042c3964adde895931a0bd628	
e0df3535d6a3936ec7e1251f16865cb06f5aa7bd28f6d974c65211ce268adef5	
e1d5ca6207213d0442faabdbbbed508006b0004f927eff5fed4ccdb8a7eda4f2	
40db93e46f69962858db63bd22f2c498b8f7121c126b359a3c7621c97ce9242b	
202c0d95606079b4f4ead96b34c80bfcf1dc5b6c6bc5fcfef4263cf14f75d52b	HTML_PHISH.AUSEID
752802b11c931f21cd6c8bb94eb4aa696339d3df4764675a30b2e2c86c4fbe23	
a5d7ee4eff49e69467459c4222b91665989bcdcb86161d03525dbe7fef6e24d9	
a93e4564d9985ae551a5fe6fa03ef814a3ede63846b0ac8b2d69c3eacd575765	

#### Hashes related to MagicApp (SHA-256) detected as IOS\_UNLOCKER.A:

Hashes
861b5d6bce3e8dd02e74c5cccfbecb0e33df70f1b6ebf63e36158593f111e061
33c6754e8ce8eb822efd91d121a98b3498873b39d82ed7bff2bfcc101d9fb694
c9924da1bf73cd2d7513bb4b5820de99a0f215c0c982c287df3d70e42e6add11
d1ece0341bd1b2168f7235e9479d9172a5d6e2e0ae48f81efc6d86b101163803
9d0205873b401808b48fc507dda45cd864f1d4d9c319d6d987d3d8ecba0fdcd2
f90647d22bc379630cc7be62d4fffe9f032c78d7016478147965ebaf080d3e32
457d3ca761905cca601c7c4bbcadcdaa56630af9353bdc388a2ff66962400a72
91ed0f1c598bdc044f5d246e7583ec3a7027ea8e62bc69a41c790ae3deb17963
40537c47078da0f8dd5aa967f859538f7d4f60358f1465ea504e8339608d1bfc
281647c9adc7fbbced290c698128aa87f33b08724ce5ecf3e8f99ed2ec460d72
f66d672becb77b001c79b4a3bfc6cf89e49a6c5836c021b8dcc79b5e240aeb22





Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro<sup>™</sup> Smart Protection Network<sup>™</sup>, and are supported by over 1,200 threat experts around the

globe. For more information, visit www.trendmicro.com.

©2017 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Created by: TrencLabs Global Technical Support & R&D Center of TREND MICRO