Goodbye Memory Scraping Malware

Hold Out Till "Chip And Pin".
Weston Hecker Security Expert With KLJ

#westonhecker #skimbadsoftware
Who Am I What Do I Do What's the Talk About,

• About Me: Speaker at Defcon 22 Tons of Computer Certs, Computer Science/Geophysics
• About 11 years pen-testing, security research, Spoke at Defcon 22 Las Vegas on Burnerphone DDOS
• NERC, FFIEC, FISMA/NIST, ISO, GLBA and FDIC, Compliance audits HIPAA, Omnibus,
• Wrote custom exploits for obscure Internet service provider gear and PMS software.
• Tools of the trade “Fleet of Fake I phones” And now android variance.
• Co-writer of Skimbad Software Open source anti malware skimming software OPEN SOURCE. This talk today will be going of this new concept of protecting Data
• Pentesting for a living everything from banks, hospitals and ISP in the Mid-west. I live and work in North Dakota
• Security projects including Reverse engineering of malware and tracking software. Working on 911 Attack mitigation projects.
TEENSY 3.1 Container!!!

Build Your Own There Awesome !!!
Hit me up on Twitter or E-mail me.
START THE DEMO !!!

- This will Run while I speak
- We will check the number at the end of the Presentation
- The Graphical demonstration version is available on Skimbad.com
- Source Code and EXE are Available on GitHub
The problem of Data skimming malware/ Large Profile cases
Why do people skim data / how much does it cost
Why do people skim data / how much does it cost

<table>
<thead>
<tr>
<th>Yes</th>
<th>201</th>
<th>Canada, OH, COLUMBUS, 43240</th>
<th>DOMINION BANK</th>
<th>Barbarossa - WORLD (valid 26%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>201</td>
<td>Canada, WA, BELLINGHAM, 98226</td>
<td>TORONTO-DOMINION BANK</td>
<td>Barbarossa - WORLD (valid 26%)</td>
</tr>
<tr>
<td>Yes</td>
<td>201</td>
<td>Canada, WA, BELLINGHAM, 98226</td>
<td>TORONTO-DOMINION BANK</td>
<td>Barbarossa - WORLD (valid 26%)</td>
</tr>
<tr>
<td>Yes</td>
<td>201</td>
<td>Canada, MI, FORT GRATIOT, 48059</td>
<td>TORONTO-DOMINION BANK</td>
<td>Barbarossa - WORLD (valid 26%)</td>
</tr>
<tr>
<td>Yes</td>
<td>201</td>
<td>Canada, MI, FORT GRATIOT, 48059</td>
<td>TORONTO-DOMINION BANK</td>
<td>Barbarossa - WORLD (valid 26%)</td>
</tr>
<tr>
<td>Yes</td>
<td>201</td>
<td>Canada, AZ, GILBERT, 85296</td>
<td>TORONTO-DOMINION BANK</td>
<td>Barbarossa - WORLD (valid 26%)</td>
</tr>
<tr>
<td>Yes</td>
<td>201</td>
<td>Canada, MI, FORT GRATIOT, 48059</td>
<td>TORONTO-DOMINION BANK</td>
<td>Barbarossa - WORLD (valid 26%)</td>
</tr>
</tbody>
</table>
how its sold/used to defraud
how its sold/used to defraud

- Carding/ Ordering things online
- Duplicating cards and using them in stores.
- ATM Cashout runs / Pin Skimmed Data.
- Theft of resources / Gas Food.
- Theft of online services or Licenced materials / Digital Movies /subscriptions to sites.
- Using Card data to transfer money WU runs.
### How batches of data are ex-filtrated and sold

<table>
<thead>
<tr>
<th>Thread / Author</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New !! DroidJack Android RAT [Cracked] for android phone hacking</td>
<td>klaudovsky</td>
</tr>
<tr>
<td>Winlocker/Cryplocktor/Torrentlocker Affiliatty/Bitcoins And make Build individual</td>
<td>convertbiz</td>
</tr>
<tr>
<td>DEXTER POS Skimming Software 2015 FORSALE!!! 4 Bitcoins</td>
<td>CCBASHUP</td>
</tr>
<tr>
<td>Citadel 1.3.5.1 Cracked By: MR BOTNET</td>
<td>Mr.BOTNET</td>
</tr>
<tr>
<td>unrecom 1.4 crack</td>
<td>faria8902</td>
</tr>
<tr>
<td>Anti-Zeus Tracker</td>
<td>Mr.BOTNET</td>
</tr>
</tbody>
</table>
How batches of data are ex-filtrated and sold

• USB devices used to jump “Air” gapped or tighter security
• Use if spearfishing campaigns
• Software is loaded on to systems by classic hacking methods USB, HID.
• Batches are pull to servers most of the time using POST requests every time a card is found in memory the malware sends the data to a Dump
• Dumps are compiled by BIN number and sold on carding pages price is determined by the banks usual Point of Sale and Debit limit.
• The validity rate is how many cards out of a 100 will work. Most batches sold on proper carding forums are 98% plus
• Two year old Target breach still has about a 10% validity Rate.
Initial POS terminal is breached and malware is loaded
As cards are swiped they now are send to a Server where they will be sold online.
For the demonstration this all will be ran on one computer normally the POS is separate from the card catching Server.

For This Demo

BLACK POS
How does malware tell credit card data from other data
Most Search Memory Using Custom Search Algorithms

Bank Of SkimBad

First 6 Digits are BIN #
4342 5712 3456 7891

Bank Identification Number

Valued Customer
It works against...

CHEWBACCA

BLACK POS

Back Off

DEXTER

BrutPOS

Rdasrv
Alina
vSkimmer
Dexter
BlackPOS
Decebal
JackPOS
Soraya
ChewBacca
BrutPOS
Backof

FREE
Other uses EX. Malware research
II. The approach to stopping Breaches / the tool
what currently exists to stop skimming/data exfiltration
how this concept would make batches unusable
how are random credit cards made what are Bins

Bank Of SkimBad

First 6 Digits are BIN #
4342 5712 3456 7891

Bank Identification Number

Valued Customer
How random card numbers are made

Bank Of SkimBad

First 6 Digits are BIN #

4342 5712 3456 7891

Bank Identification Number

Valued Customer

Check Digit
How it makes random names.
Honeypot card numbers to let them know breach has occurred.
Anti-keystroke Catching
III. How will malware evolve and how we will stay on top of it
Malware gets smarter and detects BINs from area and other methods
watch dog portions (protection from malware)
How to make batches look real

Fake Credit Card
651657674611614

Fake Credit Card
21354684651651981

Real Credit Card
871111843611514135

Fake Credit Card
24356894245813479

Fake Credit Card
461161465165767

Fake Credit Card
4245813479213546846
The Legitimate Credit Cards are Covered with Fakes
How to make fake batches (unscrubable no reversing of process)

Fake Credit Card
651657674611614

Fake Credit Card
21354684651651981

Real Credit Card
87111843611514135

Fake Credit Card
24356894245813479

Processor account banned after 10 cards declined in time frame
Real Number Hidden in 1000s of Fakes
Will Chip/Pin stop skimming?
Software is Open Source Free
Help make it better

There is no reason that this concept should not be built into every POS system
Conclusions:
Thanks for Listening

Questions Concerns?
Special Thanks to: Tim Swartz, My Family, My Work Defcon Crew for approving my topic.

Contact Information
• **Weston Hecker**
• Weston@skimbad.com
• www.skimbad.com
• Twitter @westonhecker @skimbadsoftware.