POINT-OF-SALE (POS) MALWARE: TACTICS AND STRATEGIES FOR PROTECTING CUSTOMER PAYMENT INFORMATION

Eric M. Fiterman
eric@spotkick.com
www.linkedin.com/pub/eric-fiterman/43/483/509/
Myth:
It’s hard to build targeted malware
“We don’t know the full extent of what transpired, but what we do know is that there was malware installed on our point-of-sale registers. That much we’ve established.”

- Gregg Steinhafel, Target CEO
Only a handful of people likely know all of the particulars, but the event has sent ripples throughout industry
Who hasn’t shopped at Target?
...the second-largest retailer in the U.S.
This event made security extremely personal
Although we are discussing high volume retail, the same rules apply for protecting other types of critical information.
Provisional Patent Application

Evan Spiegel
To: Reggie Brown

Hi Reggie,

I still haven’t received a copy of the provisional patent application that was filed. Can you please send me everything that you submitted to the patent office?

Thanks,
Evan
I’ve received personal notice of at least 3 data breaches in the last 3 months:

• Target
• Adobe
• University of Maryland (pending)
Point-of-Sale
(Point-of-Capture)
• A magnetic stripe reader is not a prerequisite for a POS

• If you enter credit card information into a computer, it’s a POS
Volume retail is a high frequency transaction environment
How did they get in?
“Like Target, we are a victim of a sophisticated cyber attack operation. We are fully cooperating with the Secret Service and Target to identify the possible cause of the breach and to help create proactive initiatives that will further enhance the security of client/vendor connections making them less vulnerable to future breaches.”

- Ross E. Fazio, President, Fazio Mechanical Services, Inc.
Compliance: 1

Security: 0
Olive Cardin’

http://www.youtube.com/watch?v=dh3JaTEqHB0
A credit card reader is an input device.

It’s designed to expedite payments and reduce errors.

If it’s not encrypted at the point of capture - it’s vulnerable to theft.
Target malware

Extract CC → Dump via CIFS
Point-of-Sale malwares / RAM scrapers

Malware who target Point-of-Sale devices.

Available samples
Dexter, aka Infostealer.Dexter (Symantec):
  - >>17147
  - >>18077
  - >>20380
  - >>20877
  - >>20899
  - >>20905
  - >>20924

Samples from VISA (warning: some files are legit):
  - >>17302
or build your own…
/* Get maximum address range from system info */
GetSystemInfo(&si);
/* walk process addresses */
lpMem = 0;

//Read in 1M chunks, probably slower
membuf = (char *) calloc(BUFSZ,1);

while (lpMem < si.lpMaximumApplicationAddress) {
    VirtualQueryEx( hProcess, lpMem, &mbi, sizeof(MEMORY_BASIC_INFORMATION) );
    /* increment lpMem to next region of memory */
    lpMem = (LPVOID)((DWORD)mbi.BaseAddress + (DWORD)mbi.RegionSize);

    ReadProcessMemory(hProcess, lpMem, (void *) membuf, BUFSZ, &memBytesRead);
    //_tprintf( TEXT("\n Read %d bytes from memory address %d"), memBytesRead, lpMem );  //, G

    findNames(lpMem, membuf, memBytesRead);
    //findTrackOne(lpMem, membuf, memBytesRead);
}

return false;
Example program for parsing memory — Edit

1 commit

branch: master
totalrecall /

first commit

Datacast authored just now

recall.cpp

We recommend adding a README to this repository to help give people an overview of your project.
Let’s see how it runs…
c:\Users\papajoe>totalrecall.exe

=================================
PROCESS NAME: RTouch.exe
=================================
Process ID = 0x00000D30
Thread count = 8
Parent process ID = 0x0000060C
Priority base = 8
Priority class = 32

c:\Users\papajoe>
TotalRecall gets a clean bill of health from VirusTotal
Anti-virus is a dead technology
- Hash injection (pass-the-hash) impersonation attacks are close cousins to data-stealing RAM scrapers

- If it’s sensitive and in memory - it’s vulnerable (although Address Space Layout Randomization helps a bit)
OSITOUCH Refurbished Systems.
Hardware Service for POSitouch.
Setup support for POSitouch systems.

Refurbished Positouch Terminals.
J2 520EX Terminals
J2 615 Terminals
12" Pioneer pos PXI Terminals, Win 2K, Win XP PRO, Win 98.
So what can you do?
Reduce your exposure
Sensitive data is both an asset and a liability

Get rid of it unless you absolutely, positively need it to run your business (e.g. Paypal, Stripe, etc)
Know where you sensitive data really lives, where it goes, what it touches.
Encrypt at the point of capture (P2PE)
Compliance has us lost in spreadsheets chasing hundreds of security controls

Set some basic, simple standards that you understand and can realistically address
Detection & Response
Understand how your domain infrastructure will work against you
This knowledge base article (PDF) published by BMC explains the Best1_user account is installed by the software to do routine tasks. That article states that while the Best1_user account is essentially a “system” or “administrator” level account on the host machine, customers shouldn’t concern themselves with this account because “it is not a member of any group (not even the ‘users’ group) and therefore can’t be used to login to the system.”

“The only privilege that the account is granted is the ability to run as a batch job,” the document states, indicating that it could be used to run programs if invoked from a command prompt. Here’s my favorite part:

“Perform Technical Support does not have the password to this account and this password has not be released by Perform Development. Knowing the password to the account should not be important as you cannot log into the machine using this account. The password is known internally and used internally by the Perform agent to assume the identity of the “Best1_user” account.”

I pinged BMC to find out if perhaps the password supplied in the Target malware (BackupU$r) is in fact the secret password for the Best1_user account. The company has so far remained silent on this question.

This was the hunch put forward by the Counter Threat Unit (CTU) of Dell SecureWorks in an analysis that was privately released to some of the company’s clients this week.
Although not very advanced, RAM scrapers need to be persistent:

✓ startup
✓ bootup
✓ services*
Look for the C2
Resources

• Kernelmode.info

• krebsonsecurity.com

• Dell SecureWorks*

• github.com/datacast/totalrecall