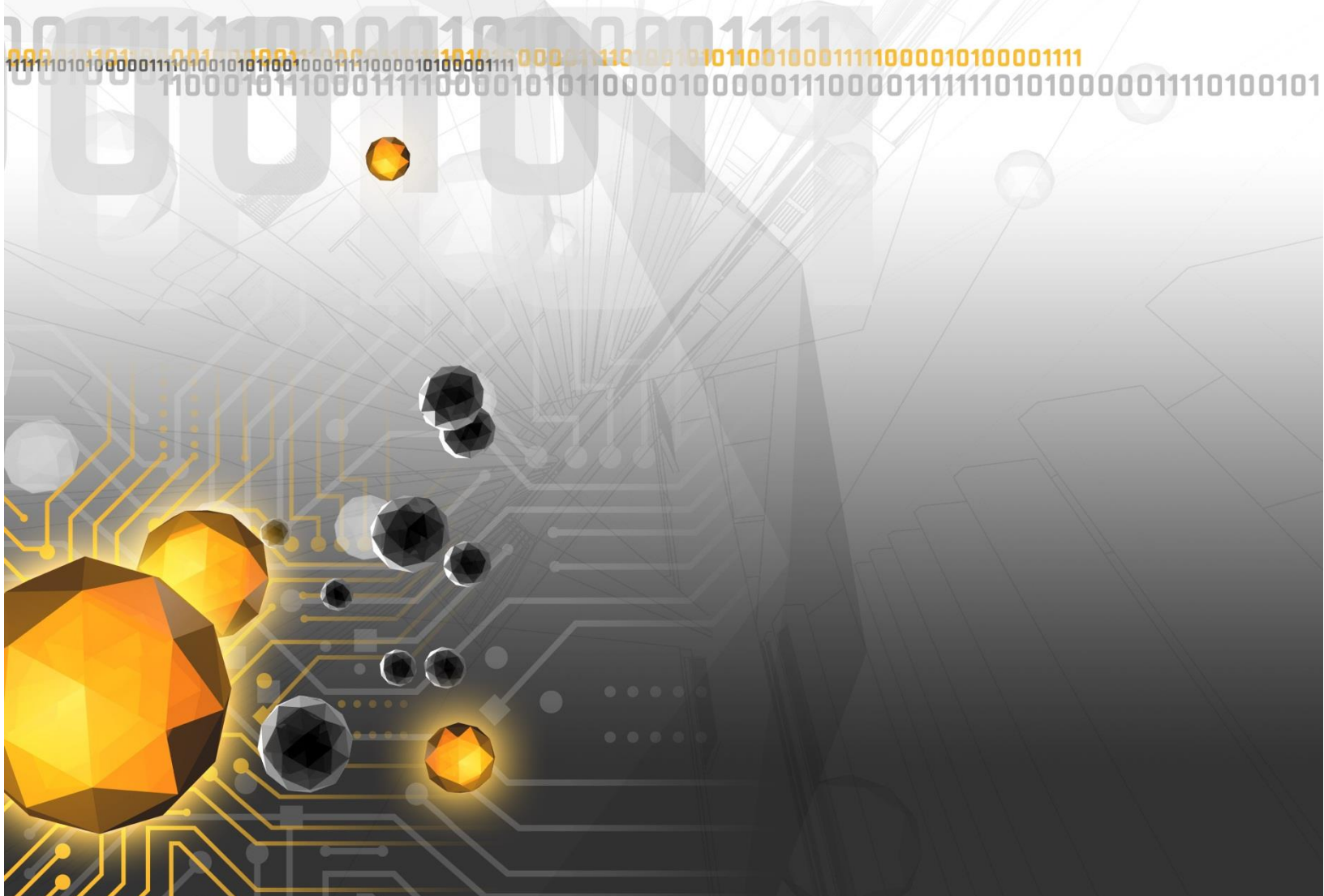
DeepSight™ INTELLIGENCE

BRUTPOS POINT-OF-SALE MALWARE TARGETS MAJOR HEALTHCARE PROVIDER, AUTOMOBILE MANUFACTURER, AND POS VENDOR IN THE UNITED STATES

MANAGED ADVERSARY AND THREAT INTELLIGENCE

DEEPSIGHT™ INTELLIGENCE | INTELLIGENCE REPORT | SYMC – 300195 | V.1
04 JUN 2015 GMT



LEGAL NOTICE

Symantec assigns a high, medium, or low degree of confidence to assessments within its DeepSight™ Intelligence Portal Managed Adversary and Threat Intelligence (MATI) products. Confidence levels are determined against a three-point spectrum of source validity: variety and non-conflictive disparity of original sources, quality of source reporting, and reliability of source reporting. Confidence levels may be increased based on independent corroboration of information. High confidence generally suggests a solid judgment can be made, though such a judgment carries the risk of being wrong. Low confidence generally suggests tenuous inferences can be made, though information used to do so may have been questionable, fragmented, or singular.

Information Cut-Off Date: 29 May 2015

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527-8000
1 (800) 721-3934
www.symantec.com

To learn more go to www.symantec.com or connect with Symantec at: go.symantec.com/social/.

BrutPOS Point-of-Sale Malware Targets Major Healthcare Provider, Automobile Manufacturer, and POS Vendor in the United States

DeepSight™ Intelligence | Intelligence Report | SYMC – 300195 | V.1 | 04 June 2015 GMT

KEY FINDINGS

- Symantec discovered multiple BrutPOS point-of-sale (POS) malware campaigns targeting a large US healthcare provider, a major US automobile manufacturer, and a large US POS vendor between March and December 2014.
- BrutPOS exploits vulnerability within a victim's Remote Desktop Protocol (RDP) over TCP/UDP port 3389. Once compromised, BrutPOS initiates brute force password-cracking techniques against the victim's POS terminal.

EXECUTIVE SUMMARY

In April 2015, while researching point-of-sale (POS) malware campaigns directed at a POS system vendor, Symantec discovered multiple BrutPOS malware campaigns occurring between March and December 2014 that targeted a large US healthcare provider, a major US automobile manufacturer, and a large US POS vendor that provides services to different businesses in multiple sectors. POS vendors are desirable targets for POS malware campaigns because of the easy attainability of their hardware and software configurations as well as their stored customer information, which actors can use in follow-on attacks against those customers. It is likely the BrutPOS attackers obtained the vendor's customer information, which may have included the healthcare provider's software and hardware configurations and default passwords. The US automobile manufacturer operates a customized POS system hosted on their own network and gaining unauthorized access to that network could compromise thousands of customers' credit information. Unlike other well-known POS malware variants, BrutPOS exploits weak passwords on victim networks and POS systems.

DETAILS

In April 2015, while analyzing multiple POS malware samples targeting a wide variety of POS vendors, Symantec identified packetized network information (i.e., PCAP) from a BrutPOS campaign that occurred between March and December 2014 indicating that one large US POS vendor was targeted in an attack. During that same time period, the configuration files from additional BrutPOS samples showed targeted IP address net blocks belonging to a large US healthcare provider and a major US automobile manufacturer.

The successful compromise of a POS vendor can yield specific customer information and allow attackers access to hardware and software configurations, including network topology and default system passwords. Symantec assesses with a high degree of confidence that the attackers targeted the POS vendor to gain access to their customer database and corresponding hardware and software configurations, including default passwords.

Symantec also assesses that the targeted healthcare provider might have been a customer of that compromised POS vendor. If the attackers were able to penetrate the POS vendor's network and gain access to its customer database, then it is likely that other businesses, in addition to the healthcare provider, were also targeted in the same time span. If the attackers were able to gain access to the healthcare provider's POS system, it is possible that sensitive patient information including insurance information and payment information might have been compromised.

The US automobile manufacturer owns their customized in-house POS system, which is used by their global franchises. In addition to payment information, the automobile manufacturer's POS system stores information required for credit checks such as social security numbers, email addresses, physical addresses, account numbers, employment history, and payment card numbers, all of which could be used by attackers to steal money and identities as well as target individuals with additional cybercrime attacks.

How BrutPOS Works

Like other POS malware variants, BrutPOS uses a RAM scraper to steal payment card information from an organization's POS system and exfiltrate that information to command-and-control (C&C) servers. The existence of the executable file llasc.exe in the AppData directory (USERPROFILE\APPDATA\llasc.exe) indicates a machine is infected with the BrutPOS malware.

BrutPOS received its name because it attempts to access a victim's POS terminal by compromising the victim's Remote Desktop Protocol (RDP) over port 3389 and then uses the vendor's default passwords to conduct brute force password-cracking techniques. In many cases, businesses that purchase POS solutions fail to change their devices' default passwords. Symantec observed BrutPOS variants attempting to log on to victim's POS terminals using the following default passwords: pos, pos1, pos01, shop, station, hotel, atm, atm1, <*posvendorname*>1, <*posvendorname*>svc, and <p*osvendorname*>pos.

BrutPOS C&C Infrastructure

The C&C infrastructure used by multiple BrutPOS malware samples between March and December 2014 included IP addresses 62[.]109.16.195, 62[.]113.2013.37, 92[.]63.99.157, and 82[.]146.34.22.

After infection, BrutPOS used an HTTP GET request over port 3389 to connect to one of the IP addresses and obtain the executable and configuration files. Once the information was successfully harvested, the BrutPOS malware used an HTTP POST request to connect to an IP address where harvested payment card data was stored. Some malware samples were observed using the same IP address for downloading executable files as well as uploading harvested information, but in several cases the malware sample used different IP addresses for each action. Those connections can be observed in Figures 1, 2, and 3.

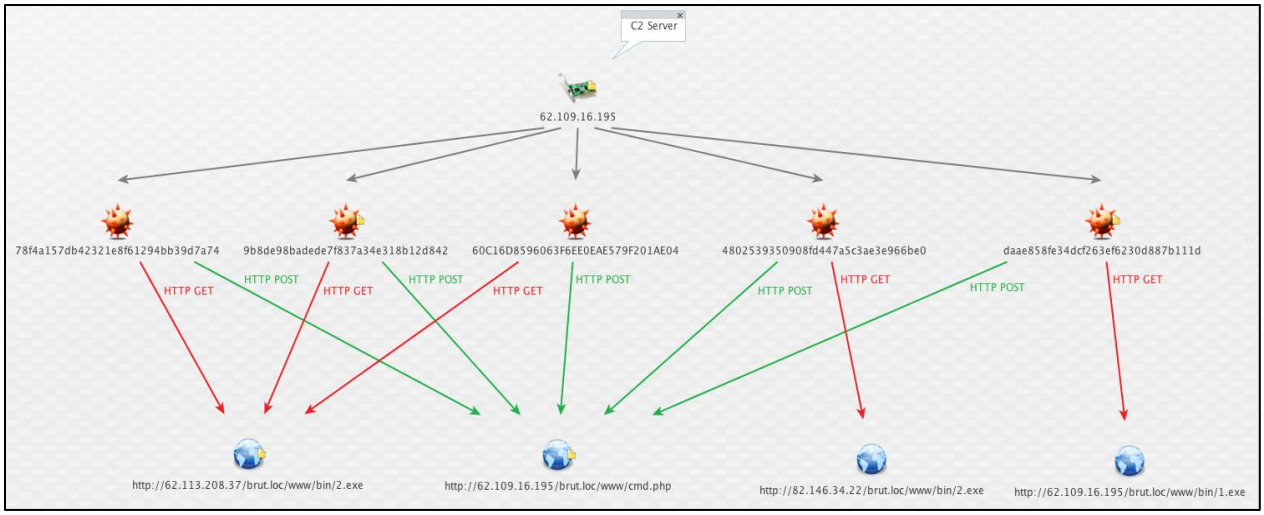


Figure 1 BrutPOS C&C server 62[.]109.16.195, Created by Symantec using Maltego®

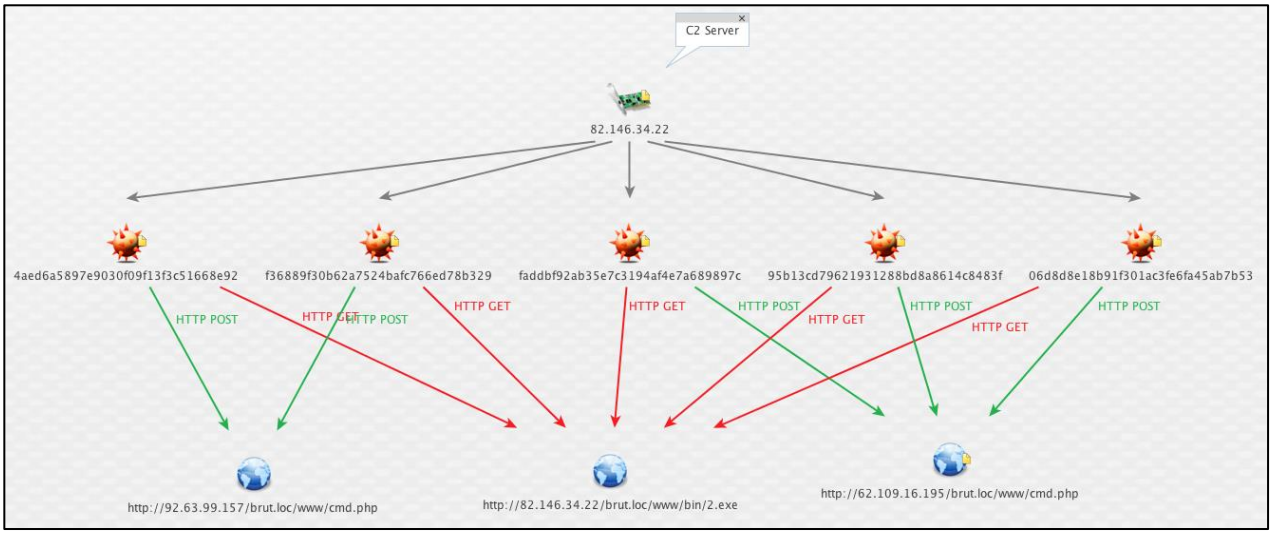


Figure 2: BrutPOS C&C server 82[.]146.34.22, created by Symantec using Maltego®

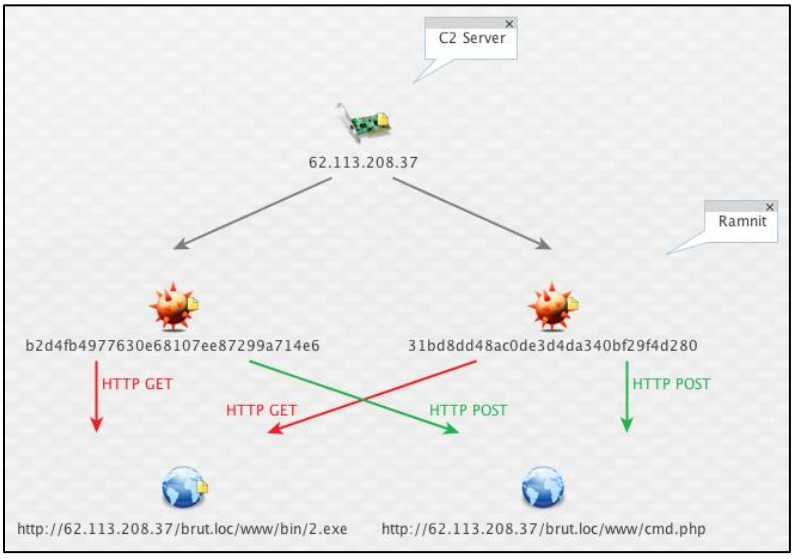


Figure 3: BrutPOS C&C server 62[.]113.208.37, a Ramnit sample was also observed using this infrastructure, created by Symantec using Maltego®

Two additional malware samples were observed using the C&C server 62[.]113.208.37 exclusively, but one of the samples was found to be the Ramnit worm (Figure 3). It is possible that in some instances the attackers were using the Ramnit worm as the initial infection vector, which would then download the BrutPOS executable. In the past, attackers used the Ramnit worm to disable many security safeguards on Windows-based systems, so it is also possible that the Ramnit worm was used to disable a target's security settings in preparation for BrutPOS.

OUTLOOK

Since January 2014, Symantec has observed several malware campaigns targeting POS vendors including a March 2015 campaign where the Vawtrak banking Trojan was used to target multiple POS vendors in Europe and the United States[i]. Symantec assesses with a high degree of confidence that those behind the March to December 2014 BrutPOS campaign were targeting the customer information and default passwords from a US-based large POS vendor. That information was then used to target the POS vendor's customers and exploit those who had not changed their default passwords.

Symantec also assesses with a high degree of confidence that actors using the BrutPOS samples to target the US automobile manufacturer may have been interested in gaining access to their proprietary POS system hosted on their network as well as customer's information used for performing credit checks, which may also be stored on the same network.

At the time of this report, the observed C&C infrastructure is no longer active and there have not been any recent BrutPOS campaigns. It is possible that the attackers behind these BrutPOS campaigns from 2014 may have moved on to a different POS malware tool. However, targeting the POS vendor and subsequently targeting their customers is evidence that businesses in the retail, healthcare, finance,

[i] See the DeepSight Intelligence report, *Two Phishing Campaigns in March 2015 Targeted Point-Of-Sale Vendors with the Vawtrak Banking Trojan* (SYMC-300188), 26 May 2015.

hospitality, and manufacturing sectors all must be aware that POS vendors are targeted by malware campaigns as well as individual businesses within those sectors. Enterprises using POS systems should factor the potential of pre-acquisition compromises of these systems into their third-party risk management plan.

TECHNICAL DETAILS

Modified Keys:

C:\Documents and Settings\Administrator\Application Data\llasc.exe
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"Run"

METADATA

Files

Detection Name	File Name	MD5	SHA256
Trojan Horse	llasc.exe	60c16d8596063f6ee0eae579f201ae04	962b6a3ec38d494697e9a214537b0b0ffbdc39542369ab5e407be036c2017b34
Trojan.Gen	DWH57A6.exe	95b13cd79621931288bd8a8614c8483f	294536030e21284c0d443cf903d3aed07fec5a424d7f00d2d99d443c0302d1f7
Trojan Horse, Suspicious.Epi	22043d83918646fdc470d1c4b6cd842402168dc77adcfbe22b9f4584141a7f96.ex$	f36889f30b62a7524bafc766ed78b329	22043d83918646fdc470d1c4b6cd842402168dc77adcfbe22b9f4584141a7f96
Trojan.Asprox.B	1375286400.exe	4aed6a5897e9030f09f13f3c51668e92	4361dfb671ecf76a9a4cba2088a2220fef36cf88077e48b3348fe9e3ecb9f6da
WS.Reputation.1, WS.Trojan.H,Suspicious.Cloud.9	1521509907.exe	faddbf92ab35e7c3194af4e7a689897c	e08536c1cb06a246d32523a6bef41073bc5a94705616ed63d8d775bd03329baa

IP Addresses

103.232.215.133
62.109.16.195
92.63.99.157
78.154.54.42
82.146.34.22
62.113.208.37
62.109.16.195
75.224.143.228
75.224.143.229
75.224.143.230
75.224.143.231
75.224.143.232

75.224.143.233
75.224.143.234
75.224.143.235
75.224.143.236
75.224.143.237
75.224.143.238
75.224.143.239
75.224.143.240
75.224.143.241
75.224.143.242
75.224.143.243
75.224.143.244
75.224.143.245
75.224.143.246
75.224.143.247
75.224.143.248
75.224.143.249
75.224.143.250
75.224.143.251
75.224.143.252
75.224.143.253
75.224.143.254
75.224.143.255
75.224.144.0
75.224.144.10
75.224.144.11
75.224.144.1
75.224.144.2
75.224.144.3
75.224.144.4
75.224.144.5
75.224.144.6
75.224.144.7
75.224.144.8
75.224.144.9

Domains and URLs

http://92.63.99.157/brut.loc/www/cmd.php
http://82.146.34.22/brut.loc/www/bin/2.exe
http://62.109.16.195/brut.loc/www/cmd.php
http://62.109.16.195/brut.loc/www/bin/1.exe
http://62.113.208.37/brut.loc/www/bin/2.exe
http://62.113.208.37/brut.loc/www/cmd.php
http://82.146.34.22/brut.loc/www/bin/1.exe
destre45.com

MD5 Hashes

06d8d8e18b91f301ac3fe6fa45ab7b53
4802539350908fd447a5c3ae3e966be0
daae858fe34dcf263ef6230d887b111d
9b8de98badede7f837a34e318b12d842
78f4a157db42321e8f61294bb39d7a74
31bd8dd48ac0de3d4da340bf29f4d280
b2d4fb4977630e68107ee87299a714e6
c0c1f1a69a1b59c6f2dab18135a73919
e38e42f20e027389a86d6a5816a6d8f8
60c16d8596063f6ee0eae579f201ae04
f36889f30b62a7524bafc766ed78b329
4aed6a5897e9030f09f13f3c51668e92
faddbf92ab35e7c3194af4e7a689897c
95b13cd79621931288bd8a8614c8483f

SHA256 Hashes

14bfda4a4aca1276388702d0fb7629af120ff34c1acdeb7613815f2981c99832
6f624fded9e83a12c8de1dd9f1ef931815c73b41379d79c4209c115e5991095e
4361dfb671ecf76a9a4cba2088a2220fef36cf88077e48b3348fe9e3ecb9f6da
e28eabeb678afb5e172f4127c5692e742809fd86dfa8478c1dc6f9c13b2a8e5f
c9842c08ba2d659257926f674ee3dcd4528e2de7c9851fc53ba076094aaeefc0
294536030e21284c0d443cf903d3aed07fec5a424d7f00d2d99d443c0302d1f7
acadb7636553efbbac9a4301efc6c4e6673c6c1f273225304d9ed378ae9f73e7
4f130a35f440fe0662b4d22844996e3f8bc74693e7c7ce69a5d4789bc36e6c4a
508909c8a00026c904f52099dd62bbf4062b4e8e40fc0601bd9e13570514b4f5
22043d83918646fdc470d1c4b6cd842402168dc77adcfbe22b9f4584141a7f96
9a10916ad0f43fa3376c2e54fd5cfdd06d684b3a19895ed4107faf9f3313dcda
962b6a3ec38d494697e9a214537b0b0ffbdc39542369ab5e407be036c2017b34
e08536c1cb06a246d32523a6bef41073bc5a94705616ed63d8d775bd03329baa

Target Industries

NAICS Code	Name
44	Retail
52	Finance and Insurance
62	Health Care and Social Assistance
31	Manufacturing

Target Regions

Region	Subregion	Countries
Americas	North America	United States

Source Regions

Region	Subregion	Countries
Europe	Eastern Europe	

Threat Domain

Cybercrime