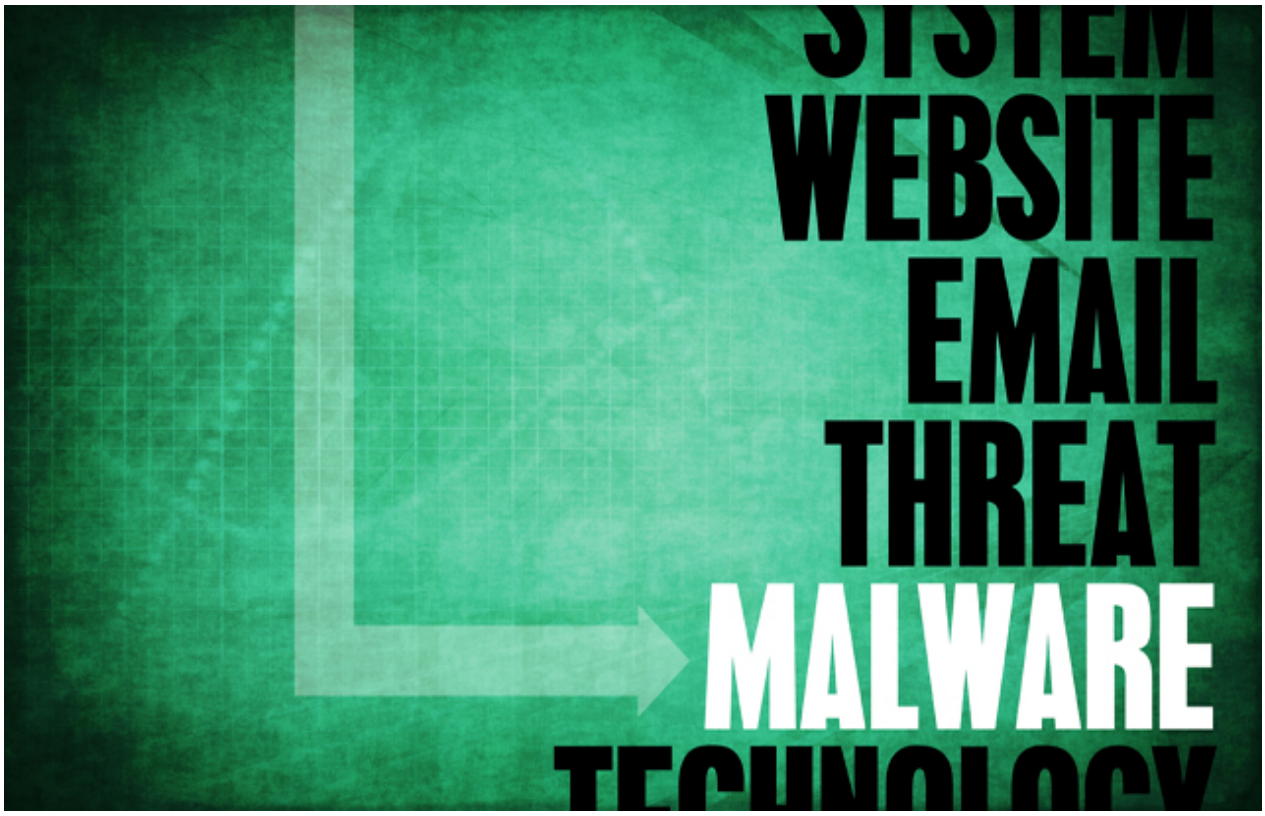
Operation Buhtrap malware distributed via ammyy.com

welivesecurity.com/2015/11/11/operation-buhtrap-malware-distributed-via-ammyy-com/

November 11, 2015



The free version of Ammyy's remote administrator software were being served a bundle that contained an NSIS installer used by the gang behind Operation Buhtrap.

Jean-Ian Boutin
11 Nov 2015 - 02:49PM

The free version of Ammyy's remote administrator software were being served a bundle that contained an NSIS installer used by the gang behind Operation Buhtrap.

We noticed in late October that users visiting the Ammyy website to download the free version of its remote administrator software were being served a bundle containing not only the legitimate Remote Desktop Software *Ammyy Admin*, but also an NSIS (Nullsoft Scriptable Installation Software) installer ultimately intended to install the tools used by the Buhtrap gang to spy on and control their victims' computers.

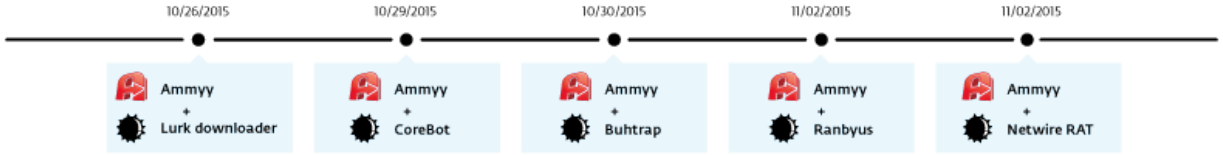
Figure 1 – Ammyy.com legitimate website

While *Ammyy Admin* is legitimate software, it has a long history of being used by fraudsters. As a result, several security products, such as ESET's, detect it as a Potentially Unsafe Application. However, it is still widely used, notably in Russia.

As noted in our previous blog on Buhtrap, this gang has been actively targeting Russian businesses, mostly through spear-phishing. It is thus interesting to see them add strategic web compromises to their arsenal. As remote administrator software is routinely used by businesses, it definitely makes sense for this gang to try to compromise visitors to this site. It's worth noting that Ammyy's website lists clients that include the top 500 Fortune companies as well as Russian banks.

The compromise

It appears Ammyy's website is now clean and serves the malware-free *Ammyy Admin* remote administrator package, but for about a week, visitors were downloading an installer that contained both malware and the Ammyy product. After investigation, different malware families were found to have been distributed through Ammyy's website. The timeline below shows which and when.



The first malware we saw was the lurk downloader, which was distributed on October 26th. We then saw Corebot on the 29th, Buhtrap on the 30th, and finally, Ranbyus and the Netwire RAT on November 2nd.

Although these families are not linked together, the droppers that might have been downloaded from Ammyy's website were the same in every case. The executable would install the real Ammyy product, but would also launch a file called either AmmyyService.exe or AmmyySvc.exe which contained the malicious payload. Thus, it is quite possible that the cybercriminals responsible for the website hack sold access to different groups.

Buhtrap

The install package behaves in exactly the same way as described in our previous blog. It first fingerprints the system by looking at software installed on the computer and at what URLs have been visited. It then downloads an additional package if the system is deemed valuable. This downloader is signed with the following certificate:

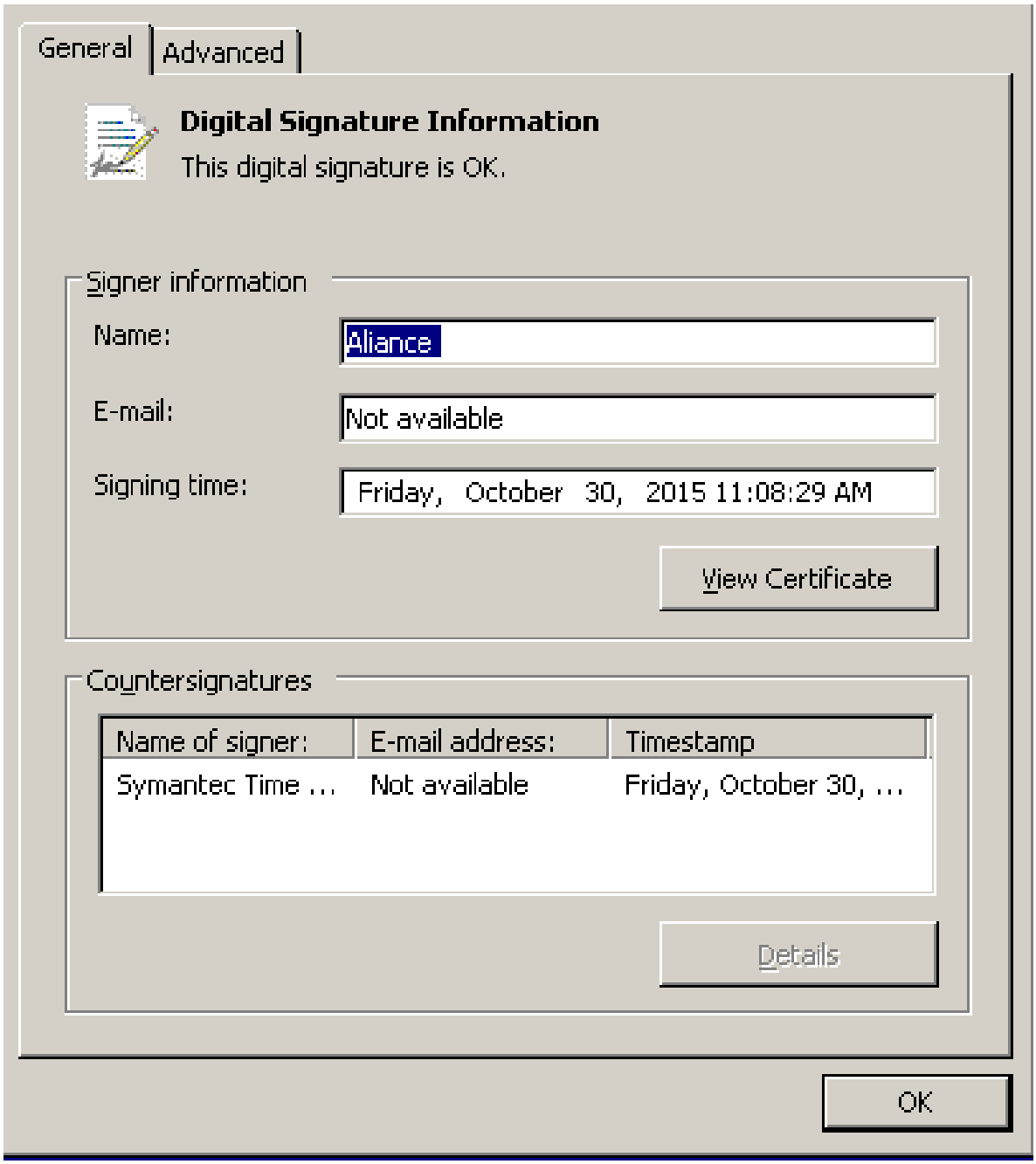


Figure 2 – Downloader's certificate

We notified Comodo which promptly revoked this certificate. The downloaded package is used to spy on the system and ultimately run code to log all keystrokes, enumerate smart cards and communicate with C&C servers. This module has exactly the same functionalities as the one that we analyzed previously and is loaded in memory through a DLL sideloading technique. The main difference this time is that the legitimate application that is used for DLL sideloading is no longer Yandex Punto, but a program called The Guide, a two-pane extrinsic outliner.

Operation Buhtrap is still ongoing and we regularly see new updates coming from the malware's authors. This group, in much the same way as the Carbanak gang, is using techniques that we are accustomed to see in targeted attacks. The fact that they now use

strategic web compromises is another sign of the closing gap between techniques used by cybercriminals and by APT actors.

If you downloaded and installed *Ammyy Admin* recently, your computer might be compromised by one of the malware described above. Since we do not know exactly when the attack started nor if the site is still compromised, we recommend that you take precautionary measures and use or install a security product to scan and protect your computer.

We tried to contact Ammyy's developers about this problem for several days and in different ways, but did not receive an answer from them. As *Ammyy Admin* is widely used, we wanted to warn its users about this security problem.

Special thanks to Anton Cherepanov, Peter Košinár and Jan Matušík for their help in this analysis.

Indicator	Value
Ammyy + Lurk downloader (Win32/TrojanDropper.Agent.REV) bundle SHA1	11657755FAD6F7B8854959D09D5ED1E0DE01D485
Ammyy + CoreBot (Win32/Agent.RLY) bundle SHA1	92CF622E997F43C208DD3835D87A9B984CE73952
Ammyy + Buhtrap (NSIS/TrojanDownloader.Agent.NSU) bundle SHA1	44769DD6A5291D1EAC79E78FEE3ED1F147990120
Ammyy + Buhtrap (NSIS/TrojanDownloader.Agent.NSU) bundle SHA1	39CE37DC0E3009E536416F5CE25C0E538CBE41E0
Ammyy + Ranbyus (Win32/Spy.Ranbyus.L) bundle SHA1	2A336AC995B6526529E01EB6303E229E40D99763
Ammyy + Netwire RAT (Win32/Spy.Weecnaw.A) bundle SHA1	10C22B70899E0F0B741C8E10964E663EBD73F4FD
Certificate thumbprint	71 49 30 ac cf 5d 9a 7f fc d7 8c 0b 58 aa a5 a7 95 38 51 be
Certificate serial number	00 8b 2f fa 23 26 66 36 f2 30 77 82 66 bb 32 41 47
Buhtrap downloaded package (Win32/RA-based.AB) SHA1	07F0B293F29EF13C61B33453E50C8C79C69BF22B
Buhtrap downloaded package URL	http://shevi-reg.com/bor/notepad.cab

11 Nov 2015 - 02:49PM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion