The Urpage Connection to Bahamut, Confucius and Patchwork

blog.trendmicro.com/trendlabs-security-intelligence/the-urpage-connection-to-bahamut-confucius-and-patchwork/

Trend Micro August 29, 2018

0

By Daniel Lunghi and Ecular Xu

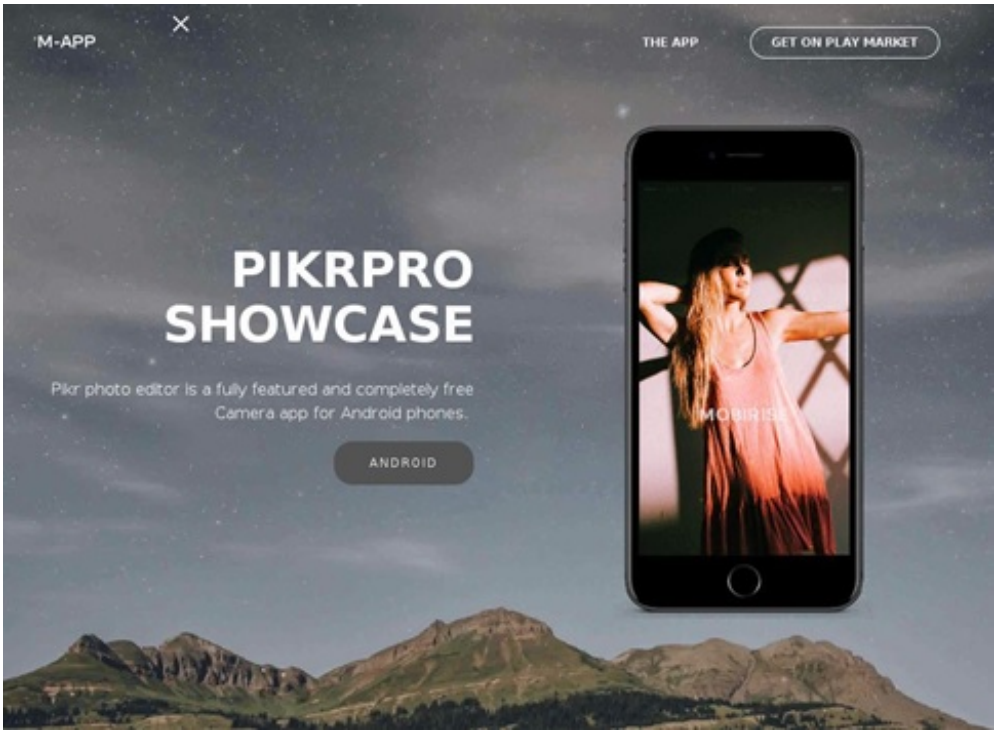
In the process of monitoring changes in the threat landscape, we get a clearer insight into the way threat actors work behind the schemes. In this case we dig deeper into the possible connection between cyberattacks by focusing on the similarities an unnamed threat actor shares with Confucius, Patchwork, and another threat actor called Bahamut. For the sake of this report, we will call this unnamed threat actor "Urpage."

What sets Urpage attacks apart is its targeting of InPage, a word processor for Urdu and Arabic languages. However, its Delphi backdoor component, which it has in common with Confucius and Patchwork, and its apparent use of Bahamut-like malware, is what makes it more intriguing as it connects Urpage to these other known threats. In our previous entry, we already covered the Delphi component in the context of the Confucius and Patchwork connection. We mentioned Urpage as a third unnamed threat actor connected to the two. This time, we look into Urpage to gain a deeper insight into the way several threat actors' actions intersect.

The Bahamut Link

Fake websites

The link between Bahamut and Urpage can be best discussed by way of the multiple malicious Android samples that matched Bahamut's code and had C&C belonging to the Urpage infrastructure. Some of these C&C websites also act as phishing sites that lure users into downloading these very applications. The threat actor sets up these fake websites describing the application and linking to the Google Play Store to download it, like in the case of the malicious website, pikrpro[.]eu, seen below



Another sample website involved the use of a closely copied version of an existing website, with slight changes in the logo and options above the page. The download links were also replaced to download the malicious Android application instead.

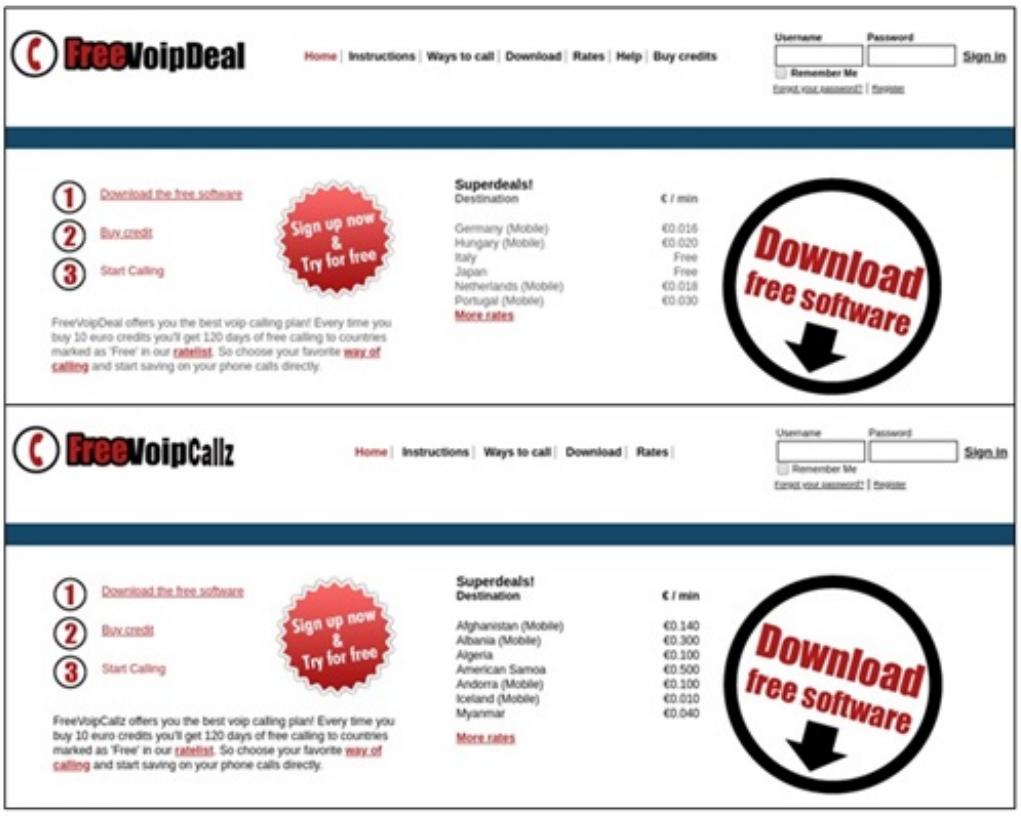


Figure 1. Original (top) and modified (bottom) website

Upon writing this entry, we've coordinated with Google to ensure that the malicious applications these C&C sites advertise are no longer available for download on the Google Play Store. It is important to note however, that not all C&C websites for Urpage advertise malicious applications. Some simply contain a random template with empty categories, likely as a ploy to hide its malicious activities.

Android targeting

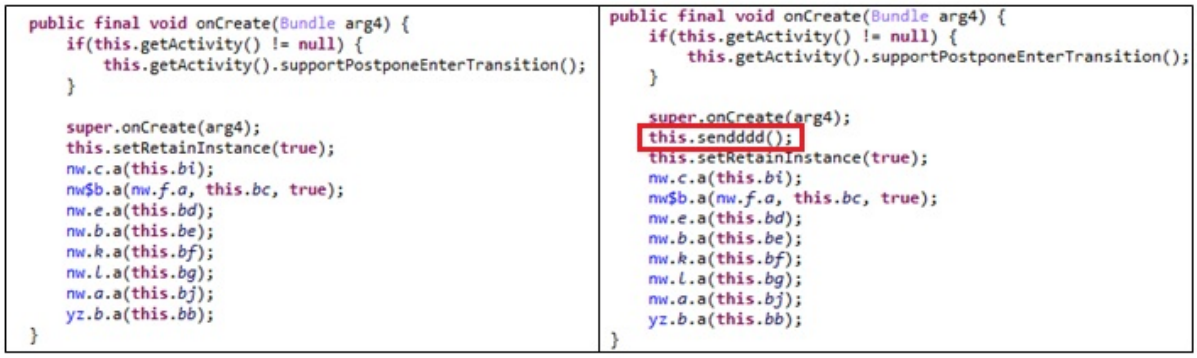
As with Bahamut applications, once downloaded and executed, it showed multiple malicious features that deal with stealing information. Some of these features are listed below.

- Retrieves basic information like network information and MAC address from an infected phone
- SMS stealing
- Contacts stealing
- Audio recording
- GPS location retrieval
- Steals files with the specific extensions, although not all samples target these extensions.

File type	File extensions
Document files	.txt, .csv, .doc, .docx, .xls, .xlsx, .pdf
WhatsApp databases	.db.crypt5 to .db.crypt12
Geolocation related files	.kml, .kmz, .gmx, .aqm
Audio files	.mp3, .opus
Videos	.mp4, .amr, .wmv, .3gp,
Pictures	.jpeg, .jpg

Of note is one specific application that had a different purpose from the others. This application has the same encryption routine as other Urpage applications. Instead of stealing documents or images, it works on top of a modified version of the legitimate Threema, an end-to-end encrypted messaging application, to steal screenshots of messages.

This application has the same icon and label as the legitimate Threema. Once launched, it drops a modified APK version of Threema and prompts the user to install the application. The malicious application then hides its icon on the device but still runs in the background, while the modified Threema works like normal. Unknown to the user, the code in the modified Threema allows it to take screenshots of itself every 10 seconds. These images are stored in the location/sdcard/Android/data/ch.threema.app/DataData directory, while the “dropper” or the malicious application working in the background uploads the images to the C&C for the threat actor to access.



```
public final void onCreate(Bundle arg4) {
    if(this.getActivity() != null) {
        this.getActivity().supportPostponeEnterTransition();
    }

    super.onCreate(arg4);
    this.setRetainInstance(true);
    nw.c.a(this.bi);
    nw$b.a(nw.f.a, this.bc, true);
    nw.e.a(this.bd);
    nw.b.a(this.be);
    nw.k.a(this.bf);
    nw.l.a(this.bg);
    nw.a.a(this.bj);
    yz.b.a(this.bb);
}
```

```
public final void onCreate(Bundle arg4) {
    if(this.getActivity() != null) {
        this.getActivity().supportPostponeEnterTransition();
    }

    super.onCreate(arg4);
    this.sendddd();
    this.setRetainInstance(true);
    nw.c.a(this.bi);
    nw$b.a(nw.f.a, this.bc, true);
    nw.e.a(this.bd);
    nw.b.a(this.be);
    nw.k.a(this.bf);
    nw.l.a(this.bg);
    nw.a.a(this.bj);
    yz.b.a(this.bb);
}
```

Figure 2. Comparison of legitimate Threema code (left) to the modified version (right) with the inserted code

Other activities

Aside from acting as a C&C and distributing Bahamut-like malware, some of these websites also serve as the host for other malicious documents. These other activities further establish the link of Urpage — and consequently Bahamut — to other threat actors.

Take, for example, the previously mentioned pikrpro[.]eu. This C&C website also acts as host not only for the malicious Android application but also for two other malicious documents listed here.

- A malicious RTF file that exploits the CVE-2017-8750 and drops a malicious VB backdoor with C&C appswonder[.]info
- A malicious InPage file that exploits CVE-2017-12824 and drops two files, one non-malicious, and one malicious VB backdoor with C&C referfile[.]com

Talos recently reported both C&C domain names with one type of campaign that targets iOS and involves MDM, and another type using VB and Delphi backdoors. This leads us back to the Confucius and Patchwork link.

The Confucius Link

In our previous entry, we already discussed how Confucius used the same Delphi file stealer as Urpage. Digging into Urpage, we found another link—two malicious RTF files that exploit different vulnerabilities but download a similar script (detected as TROJ_POWLOAD.GAA) containing two base64-encoded URLs. One of the URLs is for the decoy document, while the other one is for the payload.

One of the RTF files was found in a server related to Confucius (f1a54dca2fdfe59ec3f537148460364fb5d046c9b4e7db5fc819a9732ae0e063, detected as TROJ_CVE201711882.AG), while the other one (434d34c0502910c562f5c6840694737a2c82a8c44004fa58c7c457b08aac17bd,detected as Mal_CVE20170199-2) downloaded a VB Backdoor that pings back to twitck[.]com, a domain name belonging to Urpage.

The Patchwork Link

Patchwork also uses the Delphi file stealer as a similarity with Urpage, which suggests the

three groups are somehow related. But this link is further fortified by the Android applications we found whose code is like that of Bahamut, with the C&C matching the usual name registration pattern of Patchwork's group, as well as an infrastructure close to an old Patchwork domain. Of note was how the C&C was not encrypted in the application code, despite the fact that it contained the same encryption routines as other samples. Patchwork has also recently employed Android malware in its attacks, with its use of a customized version of AndroRAT.

Summary

The many similarities and connections show that threat actors do not work in isolation, and that attacks do not necessarily appear from out of nowhere. This may even suggest that a single development team may be behind this attack — maybe a single paid group that has sold its tools and services to other groups with different goals and targets.We've summarized all the mentioned findings in the table below.

	Urpage	**Bahamut**	**Confucius**	**Patchwork**
"BioData" Delphi backdoor and file stealer	X		X	X
VB backdoor	X			
Android "Bahamut-like" malware	X	X		X
Custom Android malware			X	
AndroRAT Android malware				X
InPage malicious documents	X		X	
simply obfuscated HTA downloaders	X		X	
IOS malware	X			
Confucius malware			X	
remote-access-c3 backdoor			X	
Sneepy/Byebye shell malware			X	
Python cloud filestealers			X	
AllaKore RAT			X	
Badnews malware				X
QuasarRAT				X
NDiskMonitor malware				X

Targets

We did not find Urpage victims in our telemetry, likely because of the targeted nature of these attacks. However, the domains used by Urpage provided hints about its target.

For one, there is the domain pikrpro[.]eu and its subdomains—the islamicfinderfeedback[.]pikrpro[.]eu and the memrifilesforinfo[.]pikpro[.]eu. The two pose as legitimate groups and websites that provide services to Islam followers and users from the

Middle East.

Additionally, many of the files related to the Urpage domains are auto-extractable files that drop Delphi or VB backdoor and open a decoy document. The decoy documents tell more about Urpage's possible targets, as it contains text from articles about the region of Kashmir. The header for a sample document can be seen below.

Office of the Spokesperson

Press Release

PM Chairs High-level meeting on Yemen situation

The documents can also be image files with the same theme, as can be seen here.

Multiple Android applications further drive this notion, as they provide services based on the interests of users in that region. They have a malicious application that provides services for religion, as well as popular sports in the region.

Figure 3. Malicious application for observing Ramadan

Figure 4. Malicious application for cricket news

Solutions and Mitigation

Taking note of these similarities and connections can help organizations and users in their continued defense against Urpage, Bahamut, Confucius, and Patchwork. The connection of Urpage to the other three threat actors demonstrate that cyberattacks don't exist in silos and that it hints at a circulation of knowledge and technologies that help in the continuing evolution of different malicious campaigns. Given this knowledge, organizations must be more vigilant in monitoring threats, as changes in one may mean that changes in others could follow.

Organizations can develop defenses against the social engineering component these four

threat actors have in common. Users should be able to identify the indicators of a social engineering campaign. Paying close attention to the domain name of a website before performing any further action can also help mitigate threats, including threats like Urpage that have targeted victims.

As an additional defense against the growing use of malicious mobile applications, enterprises and end users can benefit from multilayered mobile security solutions such as Trend Micro™ Mobile Security for Android™ which is also available on Google Play. Trend Micro's Mobile App Reputation Service (MARS) covers Android and iOS threats using leading sandbox and machine learning technologies. It can protect users against malware, zero-day and known exploits, privacy leaks, and application vulnerability.

For organizations, Trend Micro™ Mobile Security for Enterprise provides device, compliance and application management, data protection, and configuration provisioning. It also protects devices from attacks that leverage vulnerabilities, preventing unauthorized access to apps, as well as detecting and blocking malware and fraudulent websites.

The Trend Micro™ Deep Discovery™ threat protection platform enables organizations to detect, analyze, and respond to modern threats such as sophisticated malware, targeted attacks, and APTs.

Trend Micro™ Smart Protection for Endpoints with Maximum XGen™ security infuses high-fidelity machine learning into a blend of threat protection techniques to eliminate security gaps across user activity and any endpoint, offering the broadest possible protection against advanced attacks.

This appendix contains the latest Indicators of Compromise (IOCs) related to the different groups.