Abstract

On April 12, 2018, Radware's threat research group detected malicious activity via internal feeds of a group collecting user credentials and payment methods from Facebook users across the globe. The group manipulates victims via phishing emails to download a painting application called 'Relieve Stress Paint.' While benign in appearance, it runs a malware dubbed 'Stresspaint' in the background. Within a few days, the group had infected over 40,000 users, stealing tens of thousands Facebook user credentials/cookies. This rapid distribution and high infection rate indicates this malware was developed professionally. The group is specifically interested in users who own Facebook pages and that contain stored payment methods. We suspect that the group's next target is Amazon as they have a dedicated section for it in the attack control panel. Radware will continue to analyze the campaign and monitor the group's activity. Prior to publication of this alert, Radware has detected another variant of the malware and saw indication of this new version in the control panel.

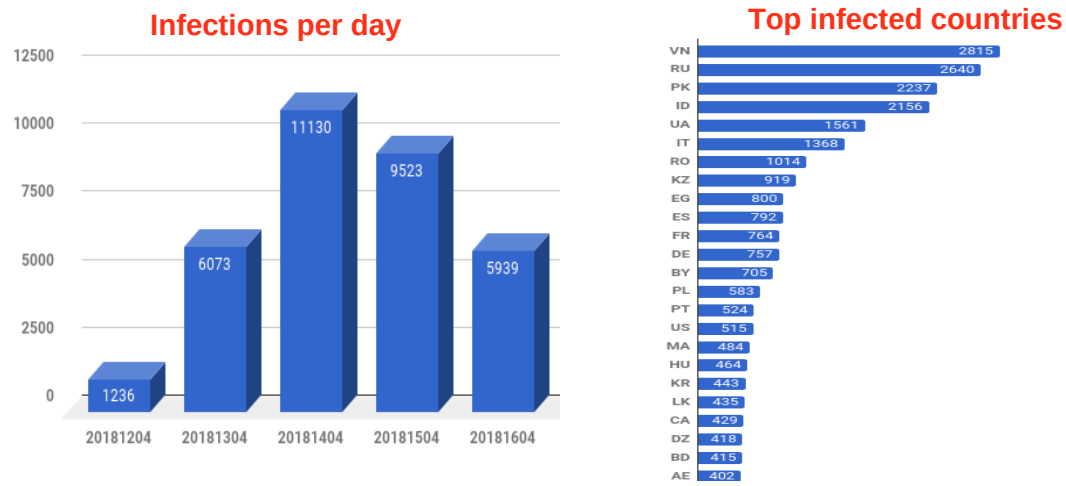

Figure 1 & 2: Breakdown of malware by infections and geographies

Infection Process

Radware suspects the infection campaign is via phishing emails or directly on Facebook itself (Radware has not yet received one). Recipients are led to believe they are going to legitimate sites (i.e. AOL) to download a legitimate application, however the site is really a Unicode domain of the AOL site.

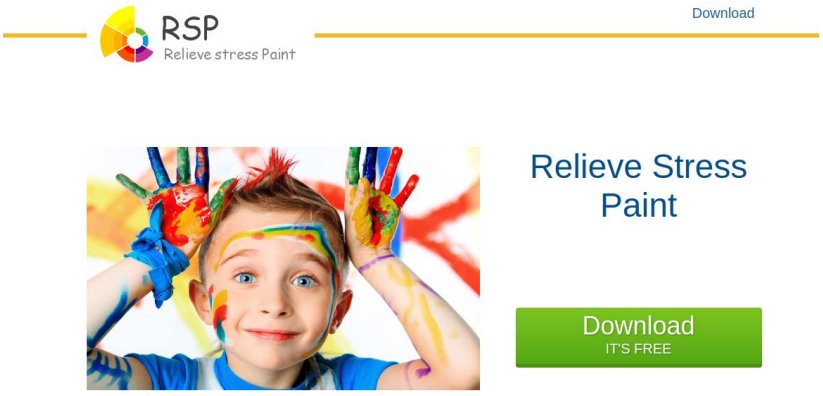

Figure 3: The phony website

The site advertises an application called “Relieve Stress Paint” and contains a download link. While the application or website are not yet visible by search engines, specific strings in the site led Radware to a site on Google called ‘aol.net.’ This is not really ‘aol.net’ but rather a Unicode representation of aol.net and its true address is **‘xn--80a2a18a.net.’**

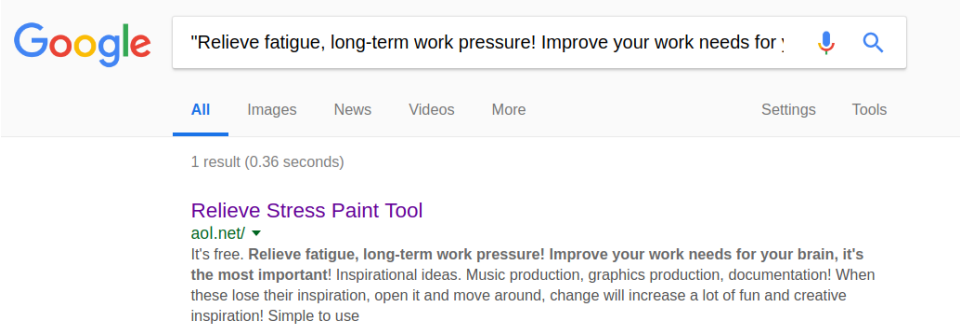

Figure 4: The malicious website as indexed by Google

The Malware

Once the file is downloaded and executed, a window is opened showing the “legitimate program” to the user. This is a paint program that changes colors and line size for each click.

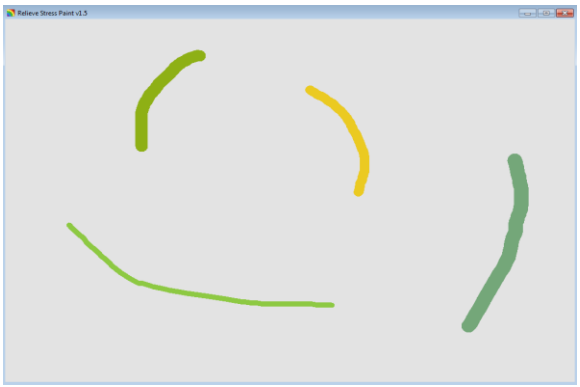

Figure 5: Screenshot of paint program

In the background, the malware immediately starts running and dropping files on the system.

- `Temp\\DX.exe –` the main module of the malware that remains persistent on the system
- `Temp\\updata.dll` - possibly used later on for credential/cookie stealing purposes
- `Desktop\RelieveStressPaint.lnk` – a desktop link to run the original downloaded executable. Supports the legitimacy of the program.
- `AppData\Local\Google\Chrome\User Data\Default\Login Data11111`
- `AppData\Local\Google\Chrome\User Data\Default\Cookies11111`
  Both are copies of the original files that are stored on the chrome folder and are used for cookies/saved password stealing and are immediately deleted

Next, a number of registry keys are also created/modified.

- `HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\Updata` - with the value of DX.exe [parameter]. We have seen two different parameters which may indicate two different infection campaigns that the author wants to track. This is also represented in the control panel.
- `HKCU\Software\Classes\VirtualStore\MACHINE\SOFTWARE\RelieveStressPaint\guid` - with the value of user GUID. This is saved in the following format [5 random letters/numbers]HHMMSSYYYYMMDD.

Afterwards, a connectivity check is done to a specific Instagram profile. Radware believes this is done to receive instructions or updates (this matter is still under investigation).

Facebook Data Theft

Information is stolen when the malware is run for the first time, if the user runs the application again (using the .lnk on his desktop), and every restart of the computer. It is done by copying the content of Chrome browser cookies and login data files to a new location and querying the data from there. Once saved login credentials (username + password) or Facebook cookies are found, they are sent encrypted to the C2 in the following format:

```
{\"fid\":\"%s\",\"fpwd\":\"%s\",\"cookies\":\"%s\",%s}
```

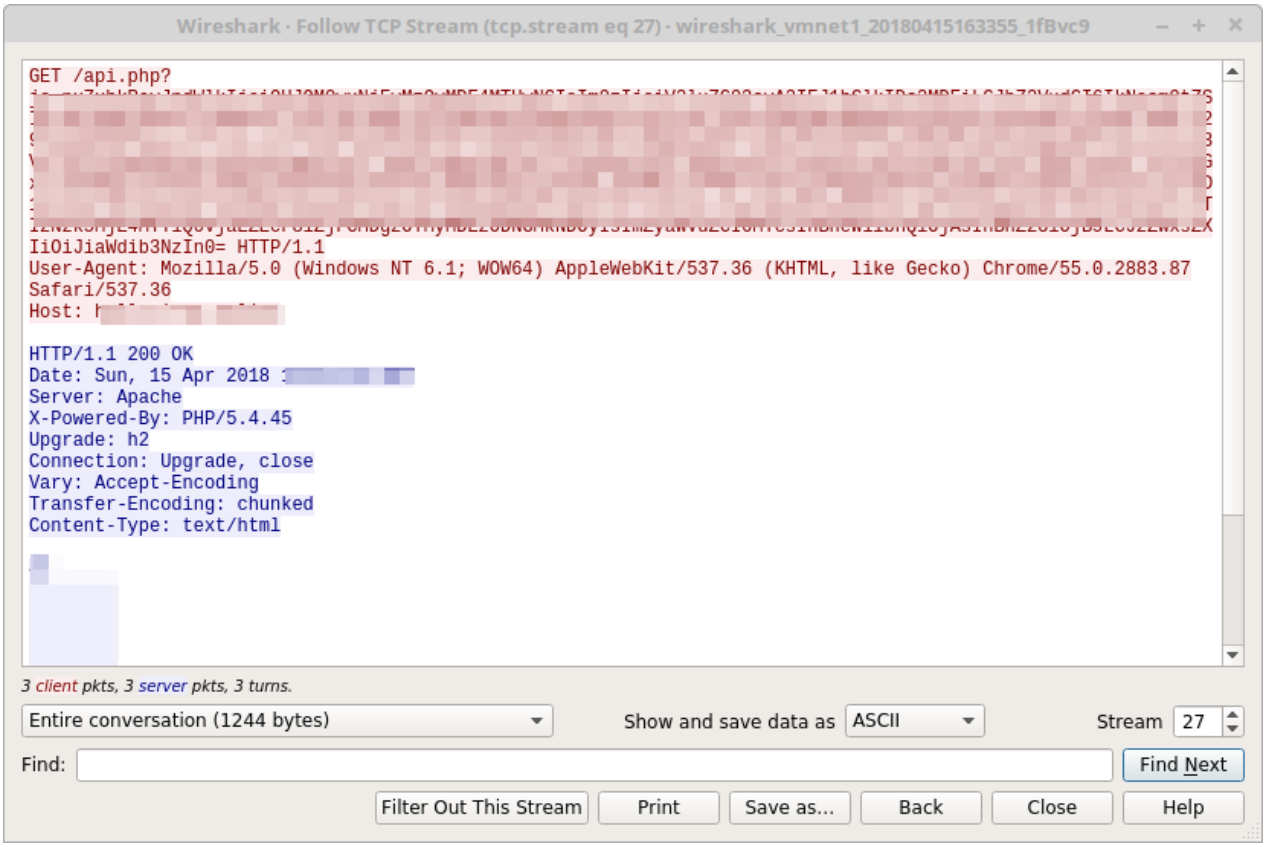

Figure 6: Exfiltration of compromised user credentials to the C&C server

On other requests, general information on the infected machine is sent in the following format:
`{\"guid\":\"%s\",\"os\":\"%s\",\"agent\":\"%s\",\"Auto\":%s,\"flag\":%s,\"data\":%s,\"seller\":\"%s\"}`

Once the credentials are validated and access is granted, additional data is collected, such as number of friends, whether the account manages a page or not, and if the payment method is configured for the account. This is done by accessing several predefined Facebook URLs which return this information. All requests are accomplished using the hard coded User agent:
`Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.87 Safari/537.36`

Stealth

The malware authors decided to leverage a specific data theft method to stay hidden on the system as long as they can.

- No general credential stealing is done which might raise some flags by security vendors
- The cookies and saved password theft is only accomplished from querying copies of the original cookies/login data files
- The process that is in charge of the credential theft resides on the system for less than a minute each time

Since they are interested only in Facebook access at this stage, they get it either from the first infection saved login/cookies or when the computer is restarted.

Control Panel

The operators of this botnet decided to use an open source Chinese CMS called Layuicms2.0. They have customized it to show information of the botnet outbreak such as stolen credentials and cookies, but also other metrics and the ability to export Facebook data. The panel also features a section for Amazon, but it is not yet functional. Radware believes that this implies that the group's next target will be Amazon.

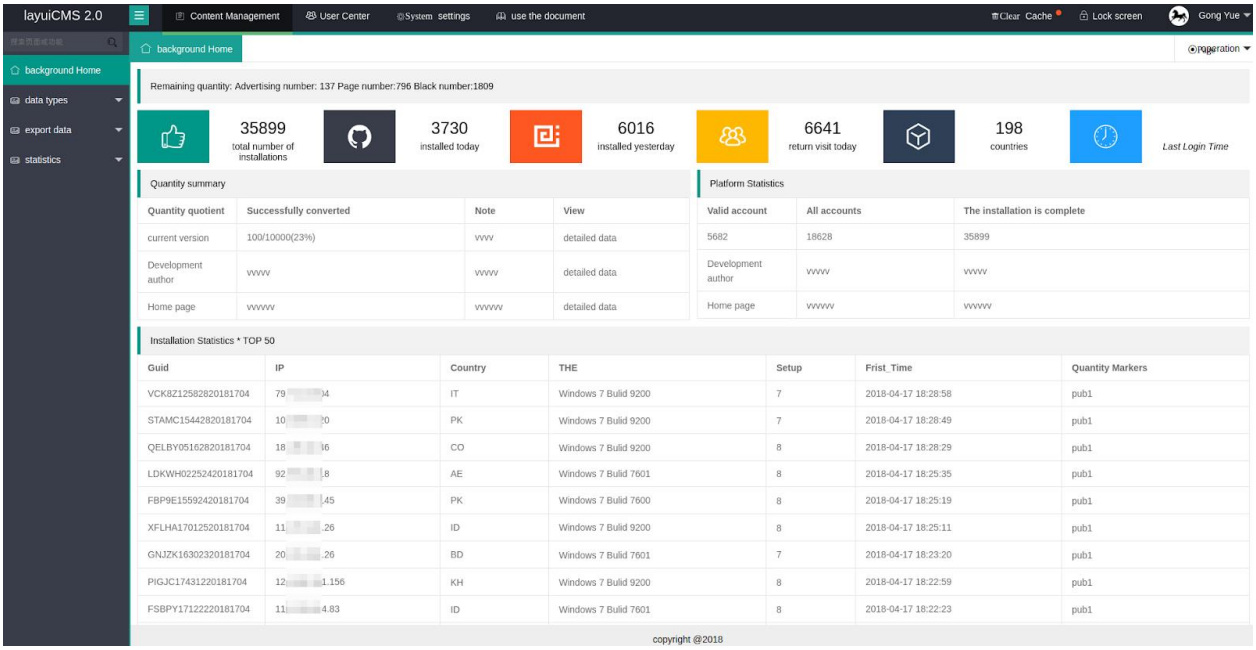

Figure 7: Control panel (translated from Chinese by Google Chrome)

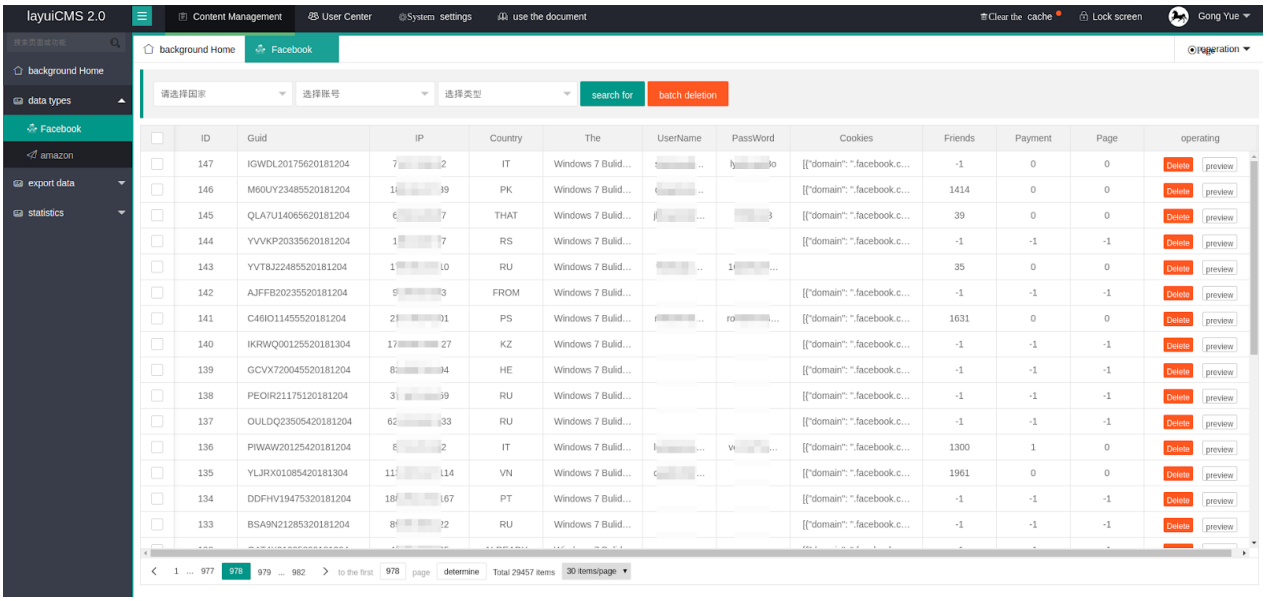

Figure 8: Users' data

Possible Impact

Since the group is at the data collection phase, Radware can only speculate what the operators of this botnet do with the stolen credentials.

- **Monetization** - simply selling stolen credentials to malicious actors and cyber-criminals. Online identities have been traded over the dark web for some time.
- **Ransom** – extort victims by threating them to reveal personal information like photos etc.
- **Espionage** - take advantage of the possessed credentials to track specific people's activity, network and conversations
- **Profit -** use the stolen credentials and payment information to shop on eCommerce sites and services
- **Identity Theft –** reuse the credentials to log-in into other accounts or services via Facebook.

However, the fact that this group is looking specifically for accounts with pages, and members with large networks, lead us to consider a couple of additional options.

- **Malvertising** – with the stolen credentials, access to web pages and payment details, the group can launch malicious advertisement campaigns, whether to make profit or spread more malwares. They can use small amounts from each user without raising suspicion and collect a critical mass to launch any activity.
- **Propaganda –** with the same information, instead of advertising a product or a service, they can run a campaign to promote their agenda and reveal people/personal identities

Steps to Protect From Data Harvesting Malwares

- Detect new zero-day malware using cutting-edge machine learning algorithms
- Block new threats by integrating with existing protection mechanisms and defense layers
- Report on malware infection attempts in your network
- Audit defenses against new exploits and see where you are vulnerable

As this malware rapidly expands, the group will certainly continue to try to find new ways to utilize the stolen assets. Such groups continuously create new malware and mutations to bypass security controls. Radware recommends individuals and organizations to update their current password and only download applications from trusted sources. Radware's Malware Research Group will keep monitoring and analyzing new threats to provide protection to its customers.

Disclosure

We have brought our research findings to the Facebook information security team, including all the stolen credentials of the accounts. Facebook is investigating this operation and has provided the following statement.

> We encourage people to check the mails they receive for trusted domains. Facebookmail.com is a common domain that Facebook uses to send notifications when we detect an attempt to log in to your account or change a password. If you're unsure if an email you received was from Facebook, you can check its legitimacy by visiting facebook.com/settings to view a list of security-related emails that have been recently sent. We are investigating these malware findings and we are taking steps to help protect and notify those who are impacted
>
> "We maintain a number of automated systems to help stop harmful links and files from appearing on Facebook and in Messenger. If we suspect your computer is infected with malware, we will provide you with a free anti-virus scan from our trusted partners. We share tips on how to stay secure and links to these scanners on facebook.com/help." – **Pete Voss, Facebook communications manager**
>
> Radware also reached out to the domain registrar to cease and decease this activity but as of time of publication received no response