MUST READ: FBI recommends that you keep your IoT devices on a separate network

# Exploit kits are slowly migrating toward fileless attacks

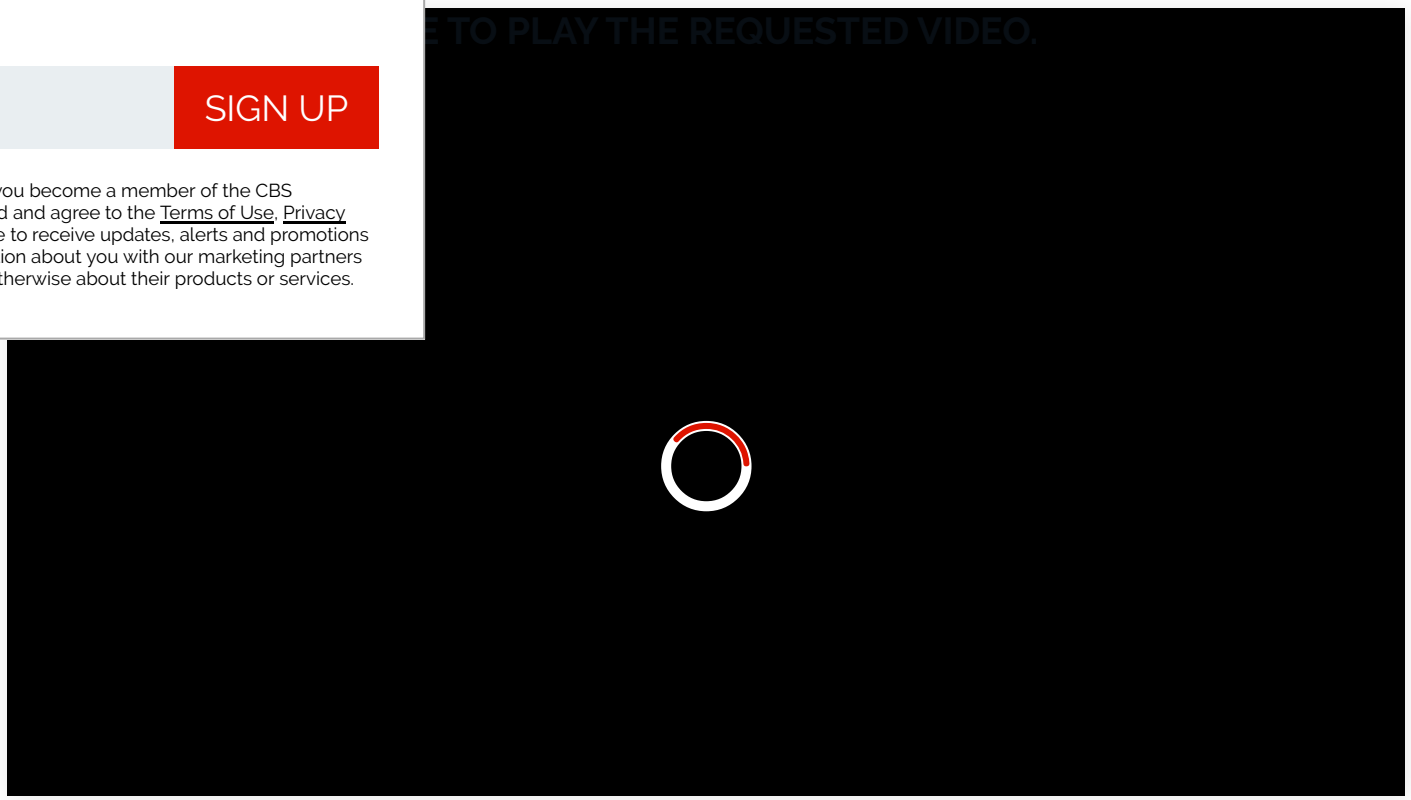
Three out of the nine exploit kits active today are using fileless attacks to infect victims.





for Zero Day | November 26, 2019 -- 05:55 GMT (21:55 PST) | Topic: Security





SEE ALSO

**10 dangerous app vulnerabilities to watch out for (free PDF)**

The malware landscape is in a constant flux, with new trends and techniques appearing and/or going out of fashion on a monthly basis.

Keeping an eye on what's what involves analyzing tens of thousands of malware samples, and this is exactly what the Malwarebytes team has been doing in terms of exploit kits, collecting and indexing campaigns and attacks for the past few years in order to get an insight into how the exploit kit landscape operates and might shift in the future.

## WHAT ARE EXPLOIT KITS?

Exploit kits, or EKs, are web-based applications hosted by cyber-criminals. EK operators usually buy web traffic from malvertising campaigns or botnet operators.

Traffic from malicious ads or hacked websites is sent to an EK's so-called "gate" where the EK operator selects only users with specific browsers or Adobe Flash versions and redirects these possible targets to a "landing page."

Here is where the EK runs an exploit -- hence the name exploit kit -- and uses a browser or Flash vulnerability to plant and execute malware on a user's computer.

## EKS ARE ADOPTING FILELESS ATTACKS

But in a report released last week, Malwarebytes researchers say EK operators are changing their tactics.

Instead of relying on dropping malware on disk and then executing the malware, at least three of the nine currently active EKs are now using fileless attacks.

A fileless attack [1, 2] relies on loading the malicious code inside the computer's RAM, without leaving any traces on disk.

Fileless malware has been around for more than half a decade, but this is the first time EKs are broadly adopting the technique.

"This is an interesting trend that makes sample sharing more difficult and possibly increases infection rates by evading some security products," said Jérôme Segura, Malwarebytes malware analyst.

The exploit kits leveraging this technique include Magnitude, Underminer, and Purple Fox.

These are small-time exploit kits when compared to other more broadly used EKs like Spelevo, Fallout, and RIG. However, this doesn't matter. The fact that a third of today's top EKs are using fileless techniques shows a clear direction where the EK market will be going in the following months and years.

## BYE-BYE FLASH!

But this wasn't the only trend spotted by Malwarebytes. The company says that more and more exploit kits are abandoning using Flash Player exploits.

The primary reason is that Adobe Flash's market share has been going down in recent years, reaching under 8% in Google Chrome, in February 2018.

Instead, exploit kits have been dog-piling on Internet Explorer bugs, despite the fact that the browser's market share has also plummeted.

The thinking, according to Malwarebytes, is that most IE instances today are in enterprise networks, so by targeting IE users, EK operators are effectively targeting enterprise networks -- which are highly sought-after targets on the malware scene.

So, in the end, despite sounding like EK operators are wasting their time, they end up infecting the targets they wanted from the beginning.

Below is a summary of the current exploit kit landscape, based on Malwarebytes' most recent report.

| Exploit kit name | Patterns | Payload |
| --- | --- | --- |
| Spelevo | • Regularly active thanks to malvertising campaigns<br>• No recent major changes<br>• Discovered in March 2019 | PsiXBot, Gootkit, Maze |
| Fallout | • It implemented a Diffie-Hellman key exchange to prevent offline replays by security analysts. | Sodinokibi, AZORult, Kpot, Raccoon, Danabot |
| Magnitude | • Active only in South Korea<br>• Hasn't changed in months<br>• Uses fileless technique to infect victims with the Magniber ransomware<br>• Will also sometime redirect users to fake cryptocurrency exchange domains | Magniber |
| RIG | • Dropped Flash Player exploits<br>• Uses only Internet Explorer exploits | Smoke Loader, Sodinokibi, Paradise, Antefrigus |
| GrandSoft | • Not very active this fall | Ramnit |
| Underminer | • Uses fileless techniques to infect victims | Hidden Bee |
| KaiXin | • Primarily active in Asia | Dupzom |
| Purple Fox | • Uses fileless techniques to infect victims | Kpot |
| Capesand | • Developed from an older exploit kitnamed Demon Hunter.<br>• Appears to be the work of one malware author. | NjRAT |

SECURITY

**FBI warns about snoopy smart TVs spying on you**

**Remember the viral app that aged you? FBI slams FaceApp as counterintelligence threat**

**A decade of malware: Top botnets of the 2010s**

**How to prevent a ransomware attack (ZDNet YouTube)**

**Best home security of 2019: Professional monitoring and DIY (CNET)**

**How to control location tracking on your iPhone in iOS 13 (TechRepublic)**

RELATED TOPICS: SECURITY TV | DATA MANAGEMENT | CXO | DATA CENTERS

By Catalin Cimpanu for Zero Day | November 26, 2019 -- 05:55 GMT (21:55 PST) | Topic: Security

SHOW COMMENTS



MORE FROM CATALIN CIMPANU

Security
**Reddit links leak of US-UK trade documents to Russian influence campaign**

Security
**BMW and Hyundai hacked by Vietnamese hackers, report claims**

Security

**FBI recommends that you keep your IoT devices on a separate network**

Security

**New vulnerability lets attackers sniff or hijack VPN connections**

NEWSLETTERS

## ZDNet Security

Your weekly update on security around the globe, featuring research, threats, and more.

Your email address

SUBSCRIBE

SEE ALL



RELATED STORIES

1 of 3

**Reddit links leak of US-UK trade documents to Russian influence campaign**

Reddit bans 61 accounts and one subreddit for "misuse of the platform."

## BMW and Hyundai hacked by Vietnamese hackers, report claims

Hacks linked to Ocean Lotus (APT32), a group believed to operate with orders from the Vietnamese government.

## These are the worst hacks, cyberattacks, and data breaches of 2019

A slew of hacks, data breaches, and attacks tainted the cybersecurity landscape in 2019.

Visit other CBS Interactive sites:

Select Site