Dridex (Bugat v5) Botnet Takeover Operation

secureworks.com/research/dridex-bugat-v5-botnet-takeover-operation

Dell SecureWorks Counter Threat Unit™ Threat Intelligence

Tuesday, October 13, 2015 *By: Dell SecureWorks Counter Threat Unit™ Threat Intelligence*

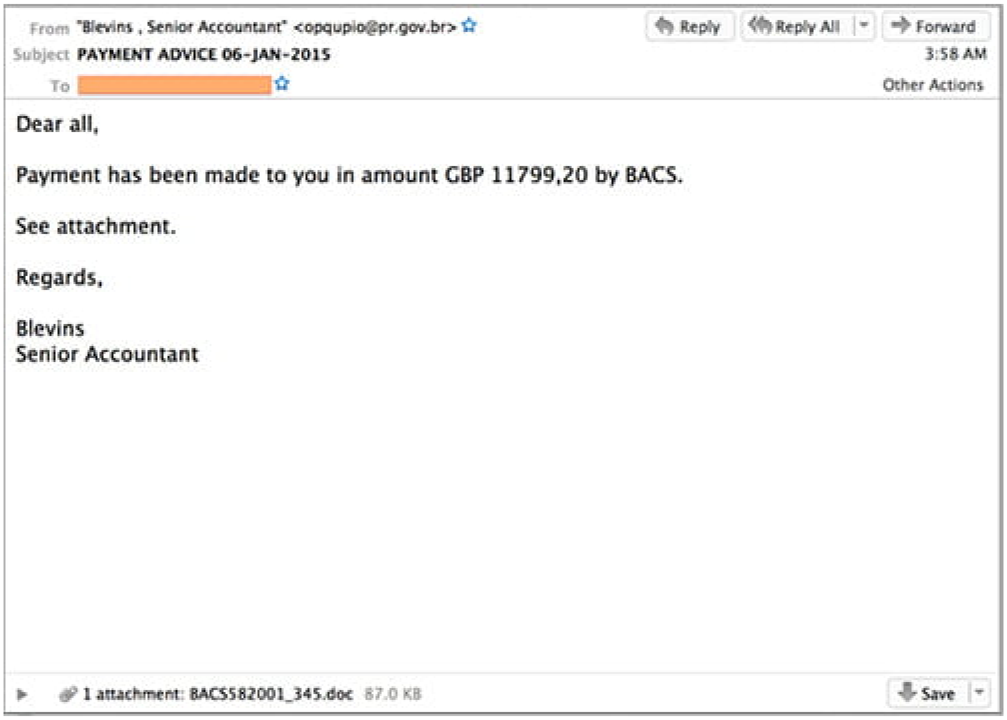
- **Author:** Brett Stone-Gross, Ph.D.
  Dell SecureWorks Counter Threat Unit™ Threat Intelligence
- **Date:** 13 October 2015

Summary

In the fall of 2015, the Dell SecureWorks Counter Threat Unit™ (CTU™) research team collaborated with the UK National Crime Agency (NCA), the U.S. Federal Bureau of Investigation (FBI), and the Shadowserver Foundation to take over the Dridex banking trojan. The malware, which the CTU research team refers to as Bugat v5, steals credentials, certificates, cookies, and other sensitive information from a compromised system, primarily to commit Automated Clearing House (ACH) and wire fraud. As of this publication, authorities have linked the botnet to an estimated £20 million (approximately $30.5 million) in losses in the UK, and at least $10 million in losses in the United States. Dridex was created from the source code of the Bugat banking trojan (also known as Cridex) but is distinct from previous Bugat variants, particularly with respect to its modular architecture and its use of a hybrid peer-to-peer (P2P) network to mask its backend infrastructure and complicate takedown attempts.

Malware distribution

Dridex is distributed through spam emails using various lures. In the past, some of the spam email attachments exploited vulnerabilities, but recent samples analyzed by CTU researchers used Microsoft Word macros (see Figure 1). After the victim opens the Word document, the macro attempts to download and execute the Dridex loader, which installs the other botnet components.



From "Blevins , Senior Accountant" <opqupio@pr.gov.br>
Subject PAYMENT ADVICE 06-JAN-2015
3:58 AM
To [redacted]

Dear all,

Payment has been made to you in amount GBP 11799,20 by BACS.

See attachment.

Regards,

Blevins
Senior Accountant

1 attachment: BACS582001_345.doc 87.0 KB

Figure 1. Spam email distributing the Dridex trojan. (Source: Dell SecureWorks)

Malware architecture

The Dridex malware has four primary components:

- Loader — downloads the core module and an initial node list to join the P2P network
- Core module — performs the malware's core functions (harvesting credentials, performing man-in-the-browser attacks using web injects, downloading the VNC and backconnect modules, etc.)
- VNC module — allows the attacker to remotely view and control a victim's computer
- Backconnect module — allows the attacker to tunnel network traffic through a victim's computer

Figure 2 shows the relationship between these modular components.

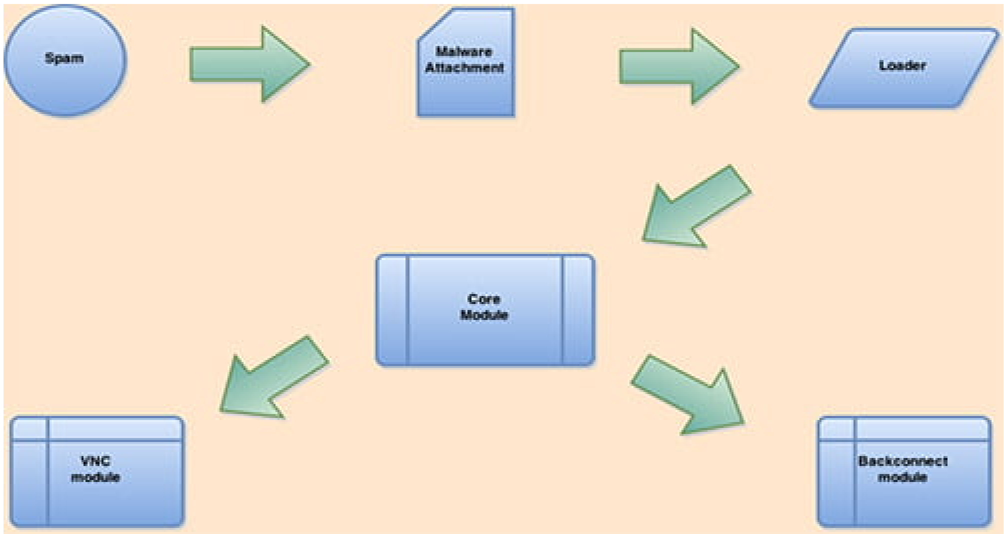


Figure 2. Architecture of the Dridex trojan. (Source: Dell SecureWorks)

Affiliate model

Similar to the P2P Gameover Zeus and Gozi Neverquest botnets, Dridex operates with an affiliate model. The botnet is partitioned into sub-botnets, and each affiliate has access to its own subset of bots. The Dridex command and control (C2) servers multiplex bot requests according to a botnet value contained in each request. CTU researchers have observed the following Dridex sub-botnets: 120, 121, 122, 125, 126, 127, 200, 220, 300, 305, 310, 320, and 888.

Botnet architecture

Early versions of Dridex (builds 0x10000 - 0x1009F) used a centralized architecture for C2 communications (see Figure 3). Like its predecessor Bugat, Dridex's compromised servers acted as proxies to the backend servers. Each Bugat/Dridex malware sample included a set of hard-coded C2 servers that the threat actors had compromised. This architecture provided a modest amount of resiliency to mitigation efforts from law enforcement and security researchers. However, this centralized architecture does not scale well and does not provide the same level of redundancy as a P2P network.

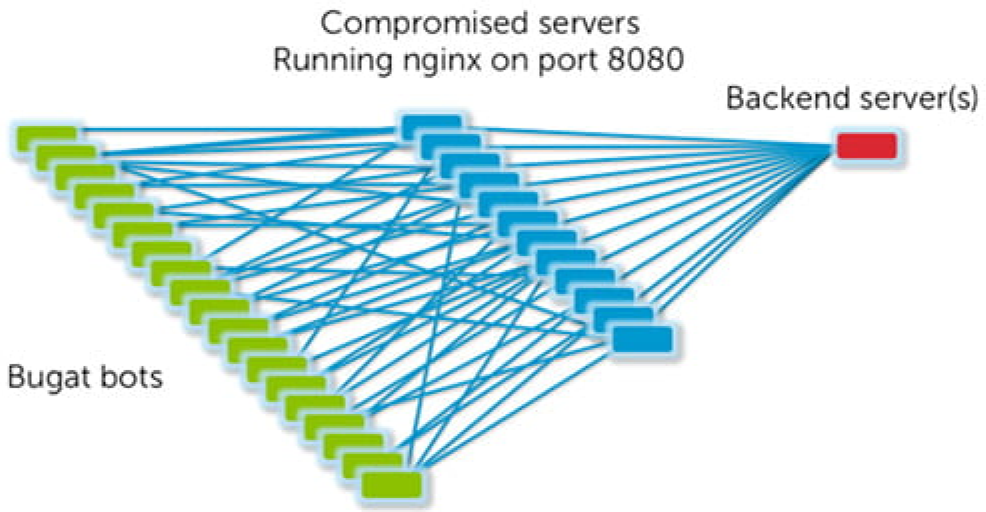


Figure 3. Botnet architecture of Bugat and early versions of Dridex. (Source: Dell SecureWorks)

Peer-to-peer communication

In November 2014, the Dridex developers for build versions greater than 0x20000 introduced a P2P network that leverages existing bots to relay traffic between bots, compromised servers, and the criminal infrastructure. Dridex bots that have a public IP address and are not behind a NAT or firewall can act as a node in a P2P network, as shown in Figure 4.

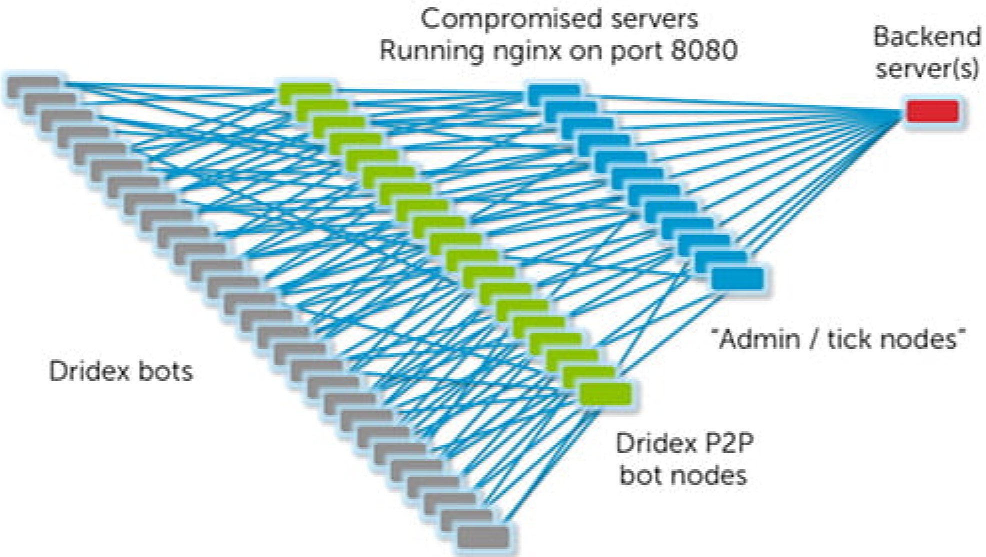


Figure 4. Revised botnet architecture for Dridex. (Source: Dell SecureWorks)

The Dridex P2P network is a hybrid between a centralized and a decentralized network. Peer lists and configuration files are distributed by the backend servers (i.e., distributed centrally) rather than exchanged directly between peers. Binary updates and modules are exchanged autonomously between peers in the network (i.e., distributed decentrally), which reduces some of the load on the backend. This hybrid P2P architecture significantly limits the botnet's ability to self-organize and maintain itself without outside intervention, unlike other P2P botnets such as Kelihos and Gameover Zeus.

Web injects

The CTU research team has tracked Dridex's activities since July 2014 and has captured 359 unique configuration files, with 414 active inject targets, as of this publication. The web injects used by Dridex vary depending on the sub-botnet, some of which are region-specific. As shown in Table 1, the Dridex botnet's web injects have targeted 27 different countries worldwide.

Region	Countries
North America	United States, Canada
Europe	United Kingdom, Ireland, France, Switzerland, Germany, Norway, Austria, Netherlands, Italy, Belgium, Croatia, Bulgaria, and Romania
Middle East	United Arab Emirates, Qatar, Israel
Asia	Indonesia, Singapore, Malaysia, Hong Kong, China, India, and Vietnam
South Pacific	Australia, New Zealand

Table 1. Regions and countries targeted by Dridex's web injects.

Dridex botnet takeover

In collaboration with the NCA, the FBI, and the Shadowserver Foundation, CTU researchers developed and executed a technical strategy to take over the Dridex botnet by poisoning each sub-botnet's P2P network and redirecting infected systems to a sinkhole. Figure 5 shows the malware infections observed at the sinkhole for Dridex's sub-botnet 220, which contained approximately 4,000 active bots. This sub-botnet heavily targeted Western Europe, especially the United Kingdom and France.

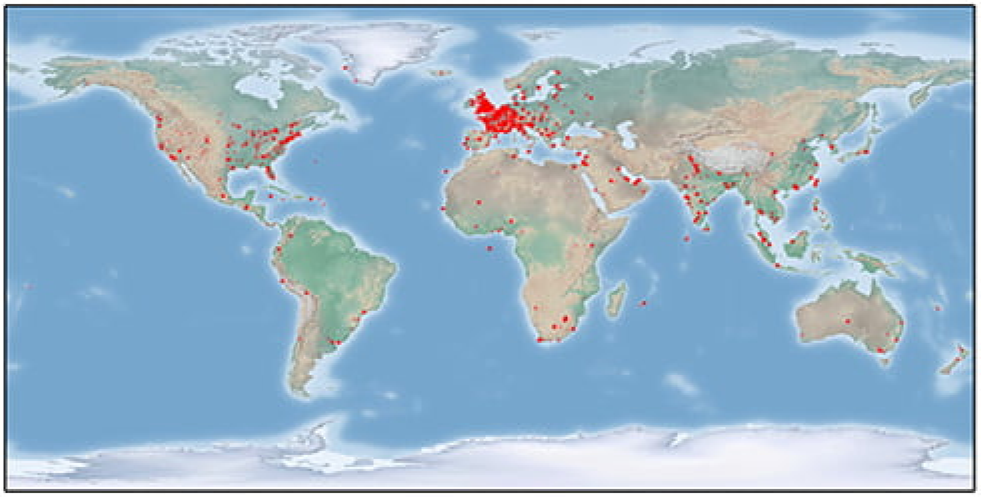


Figure 5. Map of Dridex infections for sub-botnet 220. (Source: Dell SecureWorks)

Conclusion

Threat actors created botnets such as Dridex to fill the void left by the takedown of the Gameover Zeus botnet in May 2014 as part of Operation Tovar. Despite a significant overlap in tactics, techniques, and procedures (TTPs), Dridex never rivaled the sophistication, size, and success of Gameover Zeus. This operation took advantage of weaknesses in Dridex's hybrid P2P architecture to take over the botnet.

Additional Information

National Crime Agency. "UK internet users potential victims of serious cyber attack." October 13, 2015.

The United States Department of Justice. "Bugat Botnet Administrator Arrested and Malware Disabled." October 13, 2015.