Operation Ghost: The Dukes aren’t back – they never left

By ESET Research

ESET Research

ESET researchers describe recent activity of the infamous espionage group, the Dukes, including three new malware families

17 Oct 2019 • , 8 min. read

The Dukes (aka APT29 and Cozy Bear) have been in the spotlight after their suspected involvement in the breach of the Democratic National Committee in the run-up to the 2016 US elections. Since then, except for a one-off, suspected comeback in November 2018, with a phishing campaign targeting several US-based organizations, no activity has been confidently attributed to the Dukes. This left us thinking that the group had stopped its activities.

This held true until recent months, when we uncovered three new malware families that we attribute to the Dukes – PolyglotDuke, RegDuke and FatDuke. These new implants were used until very recently, with the latest observed sample being deployed in June 2019. This means the Dukes have been quite active since 2016, developing new implants and compromising high-value targets. We call these newly uncovered Dukes activities, collectively, *Operation Ghost*.

Timeline and victimology

We believe *Operation Ghost* started in 2013 and it is still ongoing as of this writing. Our research shows that the Ministries of Foreign Affairs in at least three different countries in Europe are affected by this campaign. We have also discovered an infiltration by the Dukes at the Washington, DC embassy of a European Union country.

One of the first public traces of this campaign is to be found on Reddit in July 2014. Figure 1 shows a message posted by the attackers. The strange string using an unusual character set is the encoded URL of a C&C server used by PolyglotDuke.

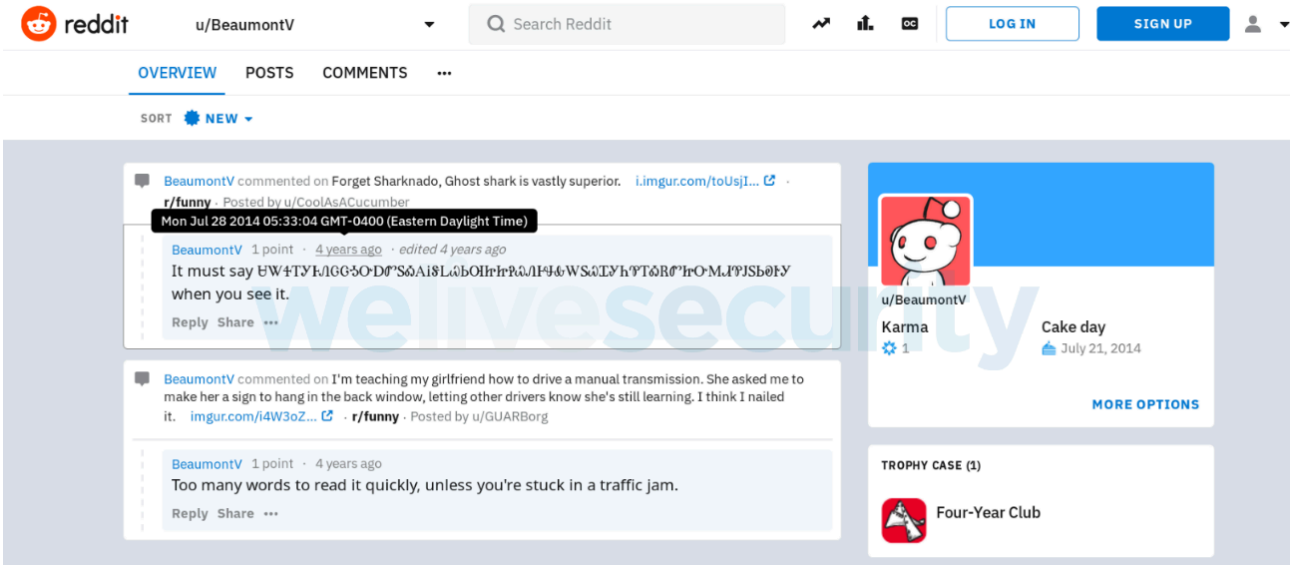

Figure 1. Reddit post containing an encoded Command & Control URL

Figure 2 presents the timeline of *Operation Ghost*. As it is based on ESET telemetry, it might be only a partial view of a broader campaign.

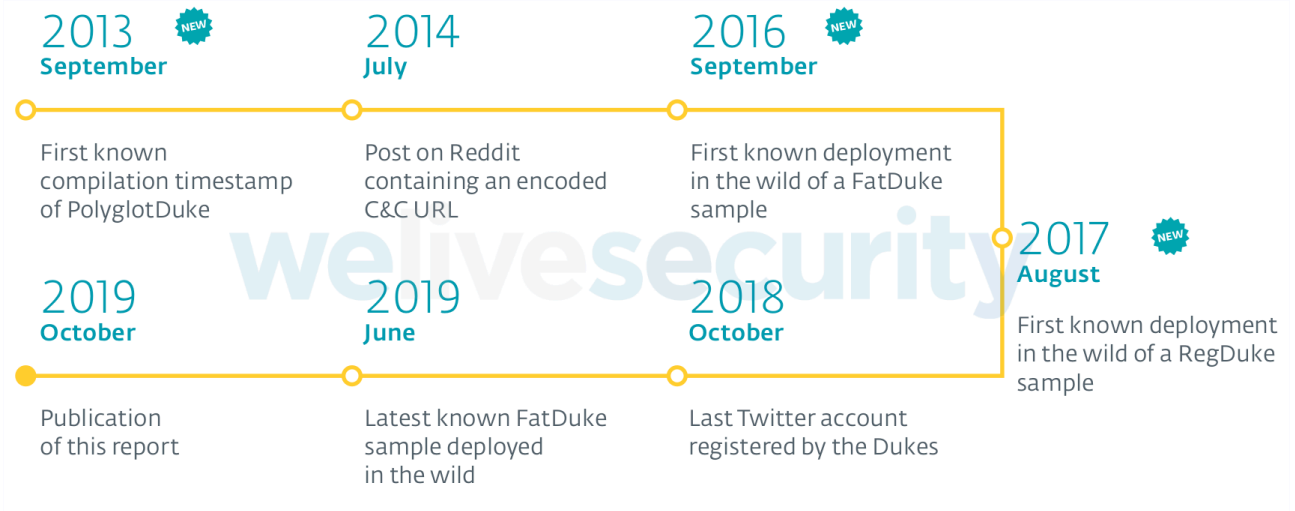

Figure 2. Timeline of Operation Ghost

Attribution to the Dukes

On one hand, we noticed numerous similarities in the tactics of this campaign to those from previously documented ones, such as the use of:

- Twitter (and other social websites such as Reddit) to host C&C URLs
- steganography in images to hide payloads or C&C communications
- Windows Management Instrumentation (WMI) for persistence

We also noticed important similarities in the targeting:

- all the known targets are Ministries of Foreign Affairs.
- known targeted organizations were previously compromised by other Dukes malware such as CozyDuke, OnionDuke or MiniDuke.
- on some machines compromised with PolyglotDuke and MiniDuke, we noticed that CozyDuke was installed only a few months before.

However, an attribution based only on the presence of known Dukes tools on the same machines should be taken with a grain of salt. We also found two other APT threat actors – Turla and Sednit – on some of the same computers.

On the other hand, we found strong code similarities between already documented samples and samples from *Operation Ghost*. We cannot discount the possibility of a false flag operation, however, this campaign started while only a small portion of the Dukes' arsenal was known. In 2013, at the first known compilation date of PolyglotDuke, only MiniDuke had been documented and threat analysts were not yet aware of the importance of this threat actor. Thus, we believe *Operation Ghost* was run simultaneously with the other campaigns and has flown under the radar until now.

PolyglotDuke (SHA-1: D09C4E7B641F8CB7CC86190FD9A778C6955FEA28) uses a custom encryption algorithm to decrypt the strings used by the malware. We found functionally equivalent code in an OnionDuke sample (SHA-1: A75995F94854DEA8799650A2F4A97980B71199D2) that was documented by F-Secure in 2014. It is interesting to note that the value used to seed the srand function is the compilation timestamp of the executable. For instance, 0x5289f207 corresponds to Mon 18 Nov 2013 10:55:03 UTC.

The IDA screenshots in Figure 3 show the two similar functions.

PolyglotDuke

```
srand(0x523BFEBBu);
SizeInBytes = (strlen(encoded_str) >> 1) + 1;
result = (char *)malloc(SizeInBytes);
Dst = result;
if ( !result )
  return result;
*result = 0;
v4 = (strlen(encoded_str) & 1) == 0;
result = (char *)encoded_str;
if ( !v4 )
  return result;
for ( i = 0; i < strlen(encoded_str); i += 2 )
{
  character = encoded_str[i + 1];
  if ( character < 48 || character > 57 )
    v7 = character - 87;
  else
    v7 = character - 48;
  v8 = encoded_str[i];
  if ( v8 < 48 || v8 > 57 )
    v9 = v8 - 87;
  else
    v9 = v8 - 48;
  Src = 16 * v9 + v7 - rand();
  if ( i == strlen(encoded_str) - 1 && Src )
    Src = 0;
  strcat_s(Dst, SizeInBytes, &Src);
}
```

OnionDuke

```
srand(0x5289F207u);
v2 = &encoded_str[strlen(encoded_str) + 1];
_SizeInBytes = ((unsigned int)(v2 - (encoded_str + 1)) >> 1) + 1;
SizeInBytes = ((unsigned int)(v2 - (encoded_str + 1)) >> 1) + 1;
if ( strlen(encoded_str) & 1 )
  return (char *)encoded_str;
result = (char *)malloc(_SizeInBytes);
Dst = result;
if ( !result )
  return result;
*result = 0;
for ( i = 0; i < strlen(encoded_str); i += 2 )
{
  character = encoded_str[i + 1];
  if ( character < 48 || character > 57 )
    v7 = character - 87;
  else
    v7 = character - 48;
  v8 = encoded_str[i];
  if ( v8 < 48 || v8 > 57 )
    v9 = v8 - 87;
  else
    v9 = v8 - 48;
  Src = 16 * v9 + v7 - rand();
  strcat_s(Dst, SizeInBytes, &Src);
}
```


Figure 3. Comparison of a custom string encryption function found in PolyglotDuke (on the left) and in OnionDuke (on the right) samples from 2013

Further, recent samples of the MiniDuke backdoor bear similarities with samples documented more than five years ago. Figure 4 is the comparison of a function in a MiniDuke backdoor listed by Kaspersky in 2014 (SHA-1: 86EC70C27E5346700714DBAE2F10E168A08210E4) and a MiniDuke backdoor (SHA-1: B05CABA461000C6EBD8B237F318577E9BCCD6047) compiled in August 2018.

MiniDuke from 2014

```
*Data = 0;
str_key_ApplicationManager = F_RC4_decrypt(&unk_407300);
if ( RegCreateKeyA(HKEY_CURRENT_USER, str_key_ApplicationManager, &phkResult) )
  return 0;
Type = 4;
cbData = 4;
str_AppId_1 = F_RC4_decrypt(&unk_407330);
if ( RegQueryValueExA(phkResult, str_AppId_1, 0, &Type, Data, &cbData) || Type != 4 )
{
  Type = 4;
  *Data = F_GetTickCount();
  str_AppId_2 = F_RC4_decrypt(&unk_407340);
  RegSetValueExA(phkResult, str_AppId_2, 0, Type, Data, 4u);
}
RegCloseKey(phkResult);
return *Data;
```


MiniDuke from 2018

```
*Data = 0;
if ( RegCreateKeyA(HKEY_CURRENT_USER, "Software\\Microsoft\\ApplicationManager", &phkResult) != 0 )
  return 0;
Type = 4;
cbData = 4;
if ( RegQueryValueExA(phkResult, "AppID", 0, &Type, Data, &cbData) || Type != 4 )
{
  Type = 4;
  *Data = F_GetTickCount();
  RegSetValueExA(phkResult, "AppID", 0, Type, Data, 4u);
}
RegCloseKey(phkResult);
return *Data;
```

Figure 4. Comparison of the same function in MiniDuke from 2014 (on the top) and in MiniDuke from 2018 (on the bottom)

Given the numerous similarities between other known Dukes campaigns and *Operation Ghost*, especially the strong code similarities, and the overlap in time with previous campaigns, we assess with high confidence that this operation is run by the Dukes.

In *Operation Ghost*, the Dukes have used a limited number of tools, but they have relied on numerous interesting tactics to avoid detection.

First, they are very persistent. They steal credentials and use them systematically to move laterally on the network. We have seen them using administrative credentials to compromise or re-compromise machines on the same local network. Thus, when responding to a Dukes compromise, it is important to make sure to remove every implant in a short period of time. Otherwise, the attackers will use any remaining implant to compromise the cleaned systems again.

Second, they have a sophisticated malware platform divided into four stages:

- PolyglotDuke, which uses Twitter or other websites such as Reddit and Imgur to get its C&C URL. It also relies on steganography in images for its C&C communication.

- RegDuke, a recovery first stage, which uses Dropbox as its C&C server. The main payload is encrypted on disk and the encryption key is stored in the Windows registry. It also relies on steganography as above.
- MiniDuke backdoor, the second stage. This simple backdoor is written in assembly. It is very similar to older MiniDuke backdoors.
- FatDuke, the third stage. This sophisticated backdoor implements a lot of functionalities and has a very flexible configuration. Its code is also well obfuscated using many opaque predicates. They re-compile it and modify the obfuscation frequently to bypass security product detections.

Figure 5 is a summary of the malware platform of *Operation Ghost*.

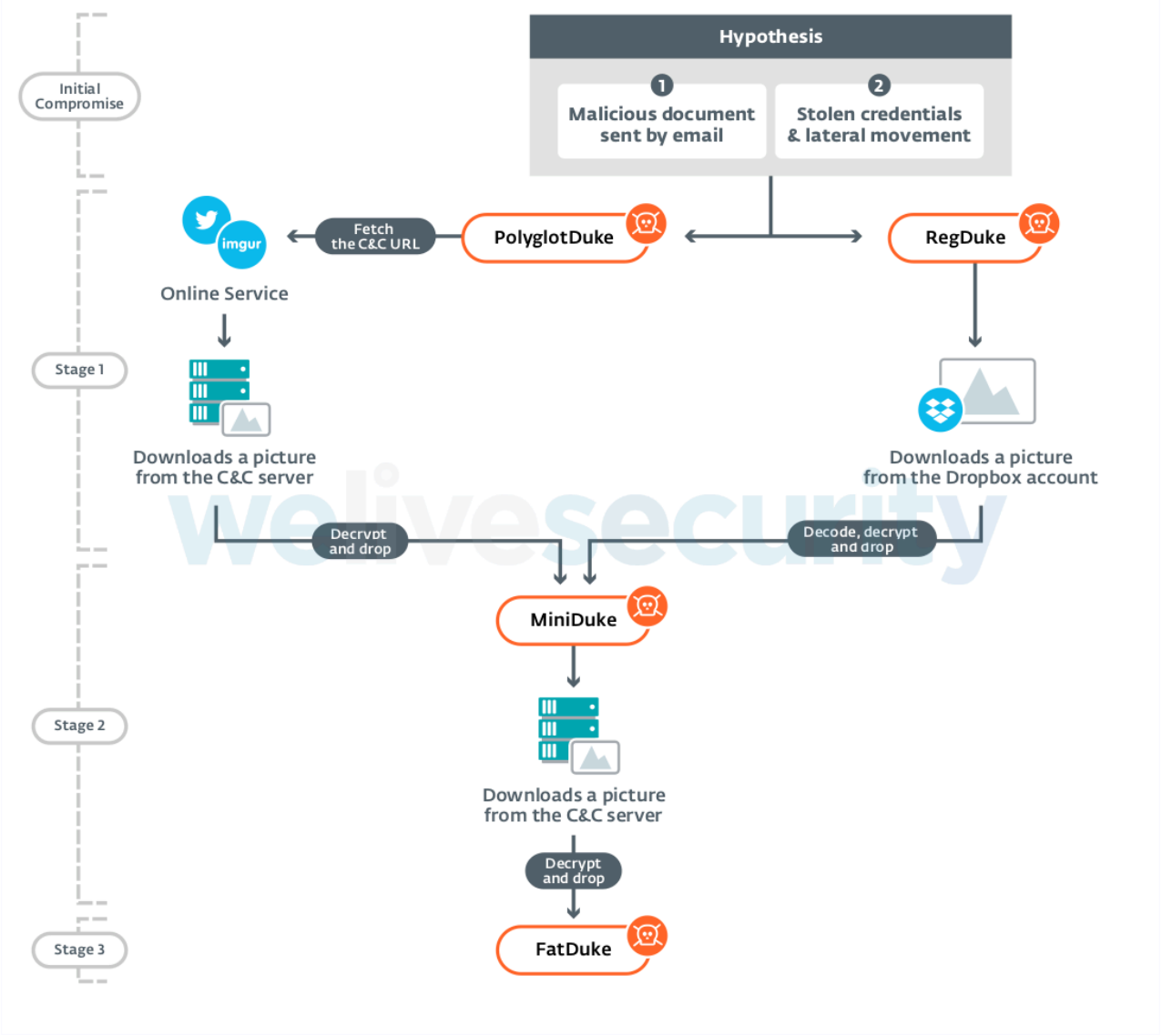

Figure 5. Summary of Operation Ghost malware platform

Third, we also noticed that the operators avoid using the same C&C network infrastructure between different victim organizations. This kind of compartmentalization is generally only seen by the most meticulous attackers. It prevents the entire operation from being burned when a single victim discovers the infestation and shares the related network IoCs with the security community.

Conclusion

Our new research shows that even if an espionage group disappears from public reports for many years, it may not have stopped spying. The Dukes were able to fly under the radar for many years while compromising high-value targets, as before.

A comprehensive list of Indicators of Compromise (IoCs) and samples can be found in the full white paper and on GitHub.

For a detailed analysis of the backdoor, refer to our white paper. *For any inquiries, or to make sample submissions related to the subject, contact us at threatintel@eset.com.*

MITRE ATT&CK techniques

Tactic	ID	Name	Description
Initial Access	T1193	Spearphishing Attachment	The Dukes likely used spearphishing emails to compromise the target.
	T1078	Valid Accounts	Operators use account credentials previously stolen to come back on the victim's network.
Execution	T1106	Execution through API	They use CreateProcess or LoadLibrary Windows APIs to execute binaries.
	T1129	Execution through Module Load	Some of their malware load DLL using LoadLibrary Windows API.
	T1086	PowerShell	FatDuke can execute PowerShell scripts.
	T1085	Rundll32	The FatDuke loader uses rundll32 to execute the main DLL.
	T1064	Scripting	FatDuke can execute PowerShell scripts.
	T1035	Service Execution	The Dukes use PsExec to execute binaries on remote hosts.
Persistence	T1060	Registry Run Keys / Startup Folder	The Dukes use the CurrentVersion\Run registry key to establish persistence on compromised computers.
	T1053	Scheduled Task	The Dukes use Scheduled Task to launch malware at startup.
	T1078	Valid Accounts	The Dukes use account credentials previously stolen to come back on the victim's network.

Tactic	ID	Name	Description
	T1084	Windows Management Instrumentation Event Subscription	The Dukes used WMI to establish persistence for RegDuke.
Defense Evasion	T1140	Deobfuscate/Decode Files or Information	The droppers for PolyglotDuke and LiteDuke embed encrypted payloads.
	T1107	File Deletion	The Dukes malware can delete files and directories.
	T1112	Modify Registry	The keys used to decrypt RegDuke payloads are stored in the Windows registry.
	T1027	Obfuscated Files or Information	The Dukes encrypts PolyglotDuke and LiteDuke payloads with custom algorithms. They also rely on known obfuscation techniques such as opaque predicates and control flow flattening to obfuscate RegDuke, MiniDuke and FatDuke.
	T1085	Rundll32	The FatDuke loader uses rundll32 to execute the main DLL.
	T1064	Scripting	FatDuke can execute PowerShell scripts.
	T1045	Software Packing	The Dukes use a custom packer to obfuscate MiniDuke and FatDuke binaries. They also use the commercial packer .NET Reactor to obfuscate RegDuke.
	T1078	Valid Accounts	The Dukes use account credentials previously stolen to come back on the victim's network.
	T1102	Web Service	PolyglotDuke fetches public webpages (Twitter, Reddit, Imgur, etc.) to get encrypted strings leading to new C&C. server. For RegDuke, they also use Dropbox as a C&C server.
Discovery	T1083	File and Directory Discovery	The Dukes can interact with files and directories on the victim's computer.
	T1135	Network Share Discovery	The Dukes can list network shares.
	T1057	Process Discovery	The Dukes can list running processes.
	T1049	System Network Connections Discovery	The Dukes can execute commands like net use to gather information on network connections.

Tactic	ID	Name	Description
Lateral Movement	T1077	Windows Admin Shares	The Dukes use PsExec to execute binaries on a remote host.
Collection	T1005	Data from Local System	The Dukes can collect files on the compromised machines
	T1039	Data from Network Shared Drive	The Dukes can collect files on shared drives.
	T1025	Data from Removable Media	The Dukes can collect files on removable drives.
Command and Control	T1090	Connection Proxy	The Dukes can communicate to the C&C server via proxy. They also use named pipes as proxies when a machine is isolated within a network and does not have direct access to the internet.
	T1001	Data Obfuscation	The Dukes use steganography to hide payloads and commands inside valid images.
	T1008	Fallback Channels	The Dukes have multiple C&C servers in case one of them is down.
	T1071	Standard Application Layer Protocol	The Dukes are using HTTP and HTTPS protocols to communicate with the C&C server.
	T1102	Web Service	PolyglotDuke fetches public webpages (Twitter, Reddit, Imgur, etc.) to get encrypted strings leading to new C&C server. For RegDuke, they also use Dropbox as a C&C server.
Exfiltration	T1041	Exfiltration Over Command and Control Channel	The Dukes use the C&C channel to exfiltrate stolen data.

Source: https://www.welivesecurity.com/2019/10/17/operation-ghost-dukes-never-left/