The stratification of cybercrime:

Using divergent TTPs to inform defensive strategies

Chester Wisniewski

Principal Research Scientist

2021 March – BSides Dublin

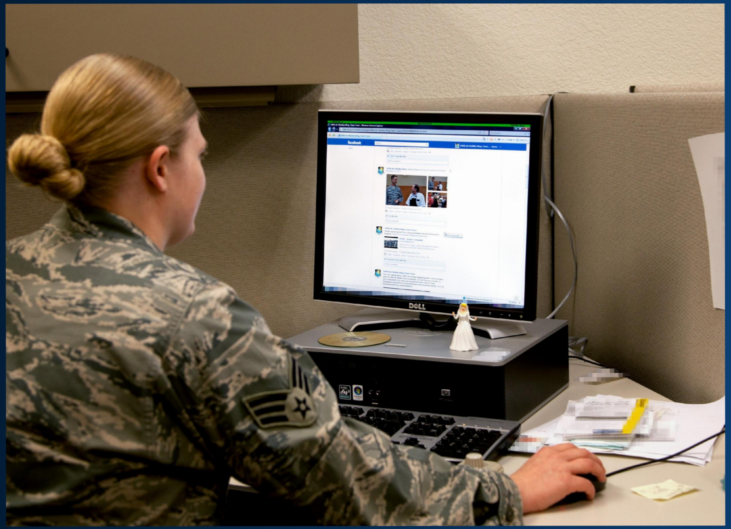
SOPHOS

The plan

- Who are our active adversaries?
- How have they gained their skills?
- What do they do that we can watch for?
- With this information, how can we define a strategy to fend them off?

Who?

Who goes there?

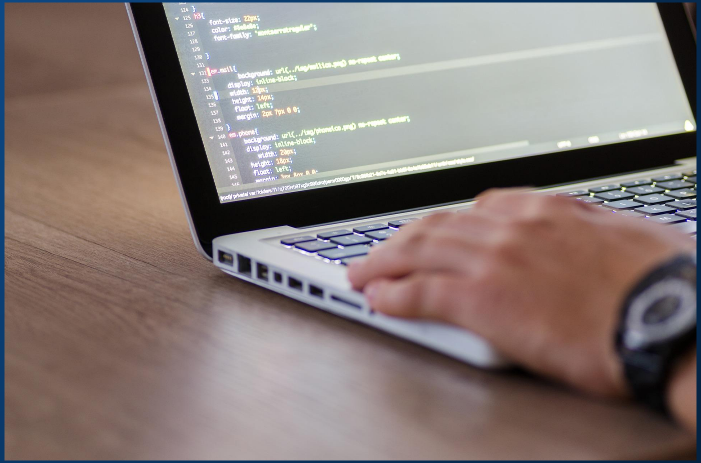


CC image courtesy of Robert Couse-Baker

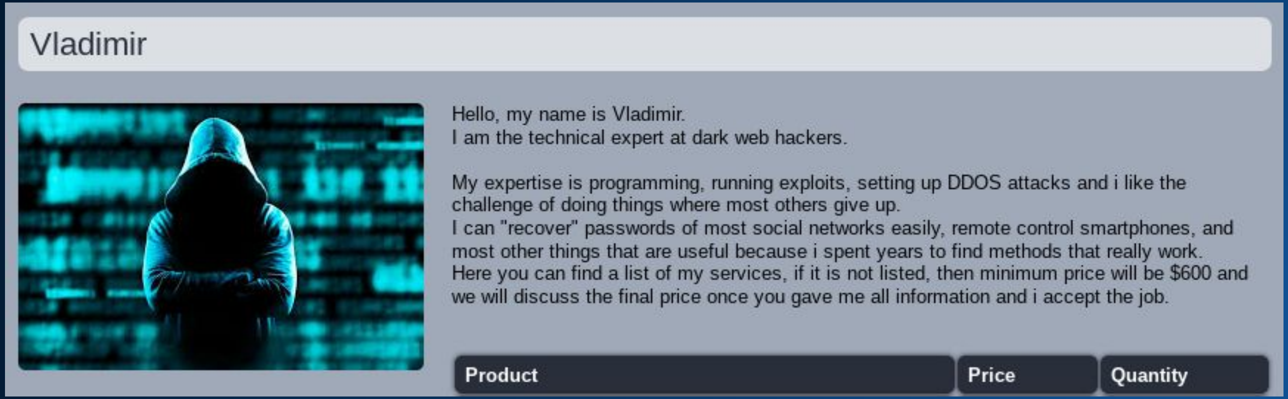
CC image courtesy of Laura D'Alessandro

How?

Advanced persistent thieves



Anything for a price

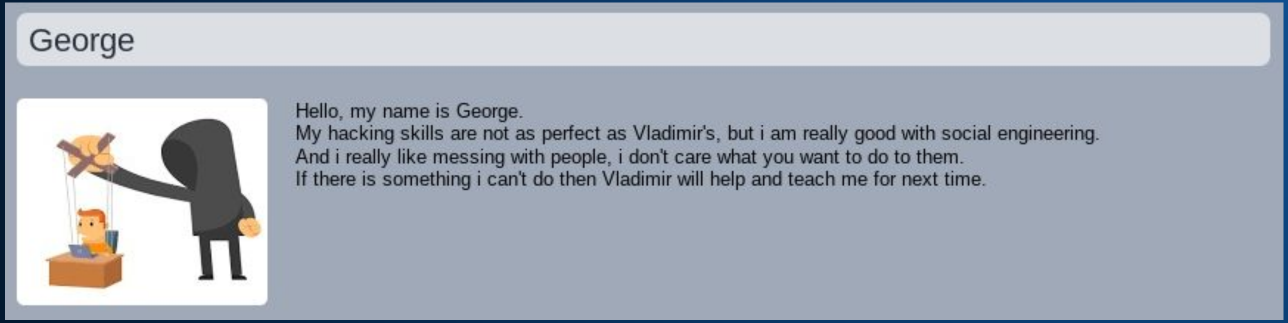


Vladimir

Hello, my name is Vladimir.
I am the technical expert at dark web hackers.

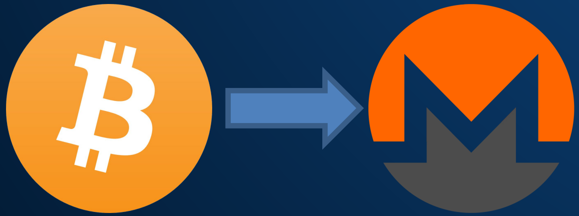
My expertise is programming, running exploits, setting up DDOS attacks and i like the challenge of doing things where most others give up.
I can "recover" passwords of most social networks easily, remote control smartphones, and most other things that are useful because i spent years to find methods that really work.
Here you can find a list of my services, if it is not listed, then minimum price will be $600 and we will discuss the final price once you gave me all information and i accept the job.

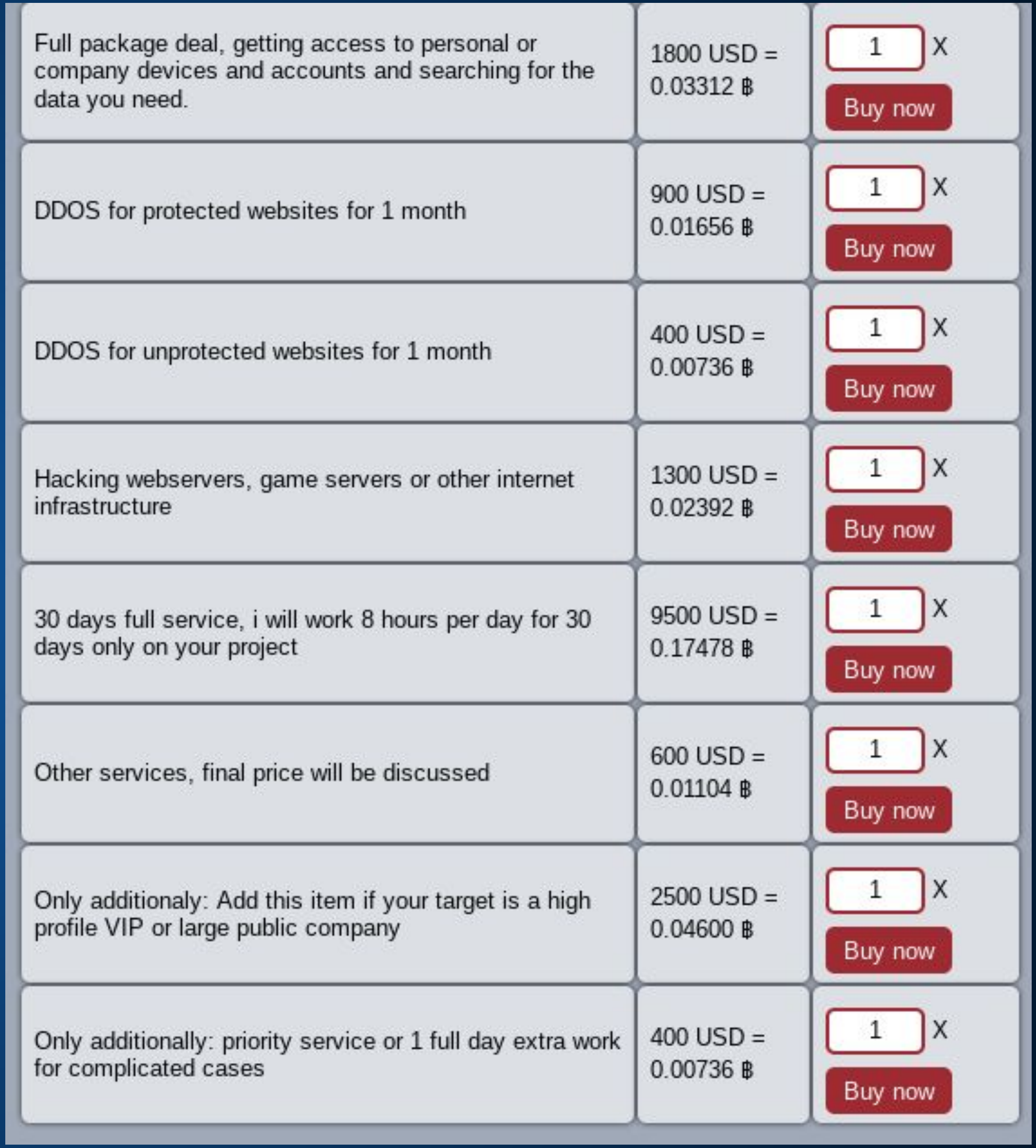
Product	Price	Quantity



George

Hello, my name is George.
My hacking skills are not as perfect as Vladimir's, but i am really good with social engineering.
And i really like messing with people, i don't care what you want to do to them.
If there is something i can't do then Vladimir will help and teach me for next time.



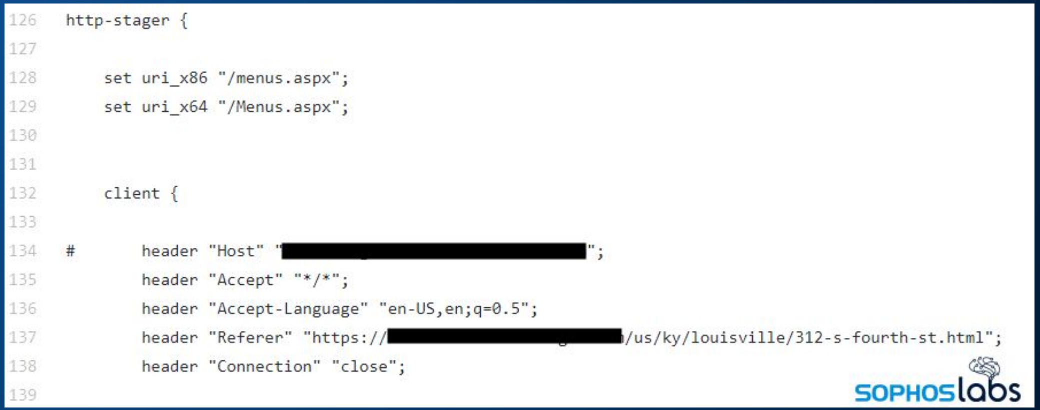


Full package deal, getting access to personal or company devices and accounts and searching for the data you need.	1800 USD = 0.03312 ฿	1 X Buy now
DDOS for protected websites for 1 month	900 USD = 0.01656 ฿	1 X Buy now
DDOS for unprotected websites for 1 month	400 USD = 0.00736 ฿	1 X Buy now
Hacking webservers, game servers or other internet infrastructure	1300 USD = 0.02392 ฿	1 X Buy now
30 days full service, i will work 8 hours per day for 30 days only on your project	9500 USD = 0.17478 ฿	1 X Buy now
Other services, final price will be discussed	600 USD = 0.01104 ฿	1 X Buy now
Only additionaly: Add this item if your target is a high profile VIP or large public company	2500 USD = 0.04600 ฿	1 X Buy now
Only additionally: priority service or 1 full day extra work for complicated cases	400 USD = 0.00736 ฿	1 X Buy now

How do they do it? (TTPs)

Example Conti attack

- Gain initial foothold (exploit, remote access)
- Cobalt Strike (#trevorforget)
- XORed loader - Meterpreter
- Cobalt Strike reflective DLL loader
- Double obfuscated, API-by-hash
- Worms over SMB while encrypting
- RSA public key in binary
- Mega.co.nz
- Dark web publish



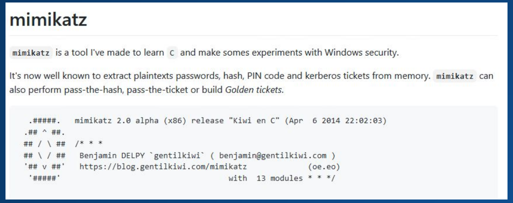
```
http-stager {

    set uri_x86 "/menus.aspx";
    set uri_x64 "/Menus.aspx";


    client {

#       header "Host" "[redacted]";
        header "Accept" "*/*";
        header "Accept-Language" "en-US,en;q=0.5";
        header "Referer" "https://[redacted]/us/ky/louisville/312-s-fourth-st.html";
        header "Connection" "close";

```

How do they ATT&CK?

Initial Access

Pulse Secure

LOLBins



mimikatz

`mimikatz` is a tool I've made to learn `C` and make somes experiments with Windows security.

It's now well known to extract plaintexts passwords, hash, PIN code and kerberos tickets from memory. `mimikatz` can also perform pass-the-hash, pass-the-ticket or build *Golden tickets*.

```
  .#####.   mimikatz 2.0 alpha (x86) release "Kiwi en C" (Apr  6 2014 22:02:03)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   https://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with  13 modules * * */
```

Windows Sysinternals

NMAP

PowerShell

Disrupt, confuse and exfiltrate

VEEAM

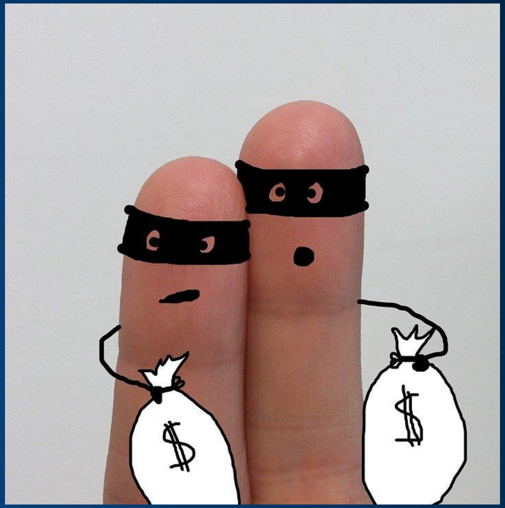
Microsoft Active Directory

End game

Best defence

Prevent

Detect, respond



SOPHOS