PRODUCT KNOWN AS	- DevilsTongue - Sourgum	Pegasus	- Predator - SpearHead	- RCS - Da Vinci, Galileo - Scout, Soldier, Elite	RCS X	KRAIT	Hermit	SWR	- Bundestrojaner - MegaPanzer - MiniPanzer	- FinFisher - FinSpy - Wingbird	- Drive Badger - Funkcjonariusz	COFEE
DETAILS LAST UPDATED	2022-06-19	2021-12-15	2022-06-18	2022-06-18	2022-06-18	2022-06-18	2022-06-18	2021-08-05	2021-08-30	2022-06-18	2022-06-18	2022-06-18
COMPANY	Candiru	NSO Group	- Cytrox Software - Amesys/Nexa Technologies - WiSpear/Passitora Ltd. - Senpai - Intellexa Alliance - Balinese Ltd., Peterbald Ltd.	HackingTeam	Memento Labs (successor of HackingTeam)	Memento Labs (successor of HackingTeam)	- RCS Lab S.p.A - Tykelab Srl		ERA IT Solutions	- Gamma Group - Elaman GmbH - FinFisher GmbH, FinFisher Labs GmbH - Vilicius Holding GmbH		Microsoft
COUNTRY	Israel	Israel	Macedonia	Italia	Italia	Italia	Italia	Russia	Switzerland / Germany	Germany	Poland	USA
AVAILABILITY	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL / NO LONGER ACTIVE, stolen and released as open source	COMMERCIAL	COMMERCIAL	COMMERCIAL	STATE	STATE, partially open sourced	COMMERCIAL	OPEN SOURCE	COMMERCIAL / NO LONGER ACTIVE
YEARS OF ACTIVITY	2014-current	2010-current	2021-current, probably developed since 2017-18	2003-2015	2018-current	2018-current	2019-current	?	2006-2011+	2008-2014+ (PC), 2018-2022 (new mobile product line)	2017-current	2008-2012
ACTIVE?	YES	YES	YES	NO - but parts forked by 3rd parties	YES	YES	YES	?	NO	NO	YES	NO
HOW IT WORKS	- remote installation - remote data interception	- remote installation - remote data interception	- remote installation - remote data interception	- remote installation - remote data interception	- remote installation - remote data interception	- remote installation - remote data interception	- remote installation - remote data interception	- remote installation - remote data interception	- local installation - remote data interception	- local installation via U3-enabled USB device - remote installation - remote data interception	- local one-time usage via USB device - local data interception - integration with 3rd party remote solutions	- local one-time usage via USB device - local data interception
SUPPORTED PLATFORMS (SUMMARY)	- Windows - Android - iOS - possibly Mac OS	- Android - iOS - Symbian - Blackberry	- iOS - possibly Android	- Windows - Mac OS - Linux - Android - iOS - Windows Mobile/Phone - Symbian - Blackberry	↩	- Android	- Android - iOS	- Windows - Linux - iOS	- Windows	- Windows - Mac OS - Linux - Android - iOS	- Windows - Mac OS - Linux - Windows Embedded - Android - iOS, iPadOS - Windows Mobile/Phone - Symbian - Canon/Nikon/HP photo cameras - VMware ESXi - Hyper-V	- Windows
HOW OPERATORS USE THE SYSTEM	- web panel for operators - all actions are logged - operators are fully responsible for any abuse attempts	- web panel for operators - all actions are logged - operators are fully responsible for any abuse attempts		- Adobe Flex panel for operators - all actions are logged - operators are fully responsible for any abuse attempts - quite easy to abuse having proper knowledge (operators got access to application source code, settings and certificate)	↩			?	?	- native Windows application panel called FinFisher HQ Software	- all exfiltrated data are stored locally on the USB device (on encrypted partition) - no panel - operator has full access to raw data and can analyze it in preferred way, eg. import into Magnet AXIOM, Paraben E3, FTK Forensic Toolkit, Autopsy, or SANS SIFT for forensic analysis using these tools - basic Linux knowledge is required - both USB device and collected data are in the sole possession of the operator - no operator abuse control	- all results are available as big html raport, stored locally on the USB device - both USB device and collected data are in the sole possession of the operator - no operator abuse control
COMMENTS REGARDING NAMING	"Sourgum" alternative name was sometimes used both as the solution name and company name, due to miscommunication between antivirus software vendors.		- "Intellexa Alliance" is a marketing name, not an oficially registered company name. - SpearHead = Predator platform + specially-outfitted van equipped with 24 antennas that can force a target's phone or computer to connect to its Wi-Fi-based interceptor at a distance of up to 1640 feet.	- Da Vinci and Galileo were separate platforms, together called RCS - Scout, Soldier, Elite - standalone parts of Galileo platform	RCS X is the direct successor of HackingTeam RCS, just updated to support new operating system versions.	KRAIT is the new Android-only platform, separate from RCS.				Wingbird is the name assigned by antivirus software vendor. The product itself was always marketed and sold as Fin* (FinFisher, FinSpy, FinFly, FinSploit, FinIntrusion etc.).	- Drive Badger - original name, international project - Funkcjonariusz - version for Poland	COFEE = Computer Online Forensic Evidence Extractor

SUPPORTED PLATFORMS AND CAPABILITIES

WINDOWS (PC)												
1. Supported versions	- 7 - 10 (documentation states that only 64-bit) - not sure about Windows 8 / 8.1 - not sure about Windows Server	n/a	n/a	- XP SP3 - 2003 - Vista - 7 - 8 (not sure about 8.1)	↩	n/a	n/a	- 7 - 8.1 (not sure about 8) - 10 - Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016, 2019	- XP (rootkit) - Vista	- 98 (very limited version) - 2000 - XP - Vista - 7 - 8 (not sure about 8.1)	- from XP SP2 to 11 (including "S") - Server 2003-2022 - Embedded Standard 7 and 2009	- XP - possibly Server 2003 32-bit
2. Software-only installation method(s)	remote installation using - CVE-2021-31979 and CVE-2021-33771 (attack on Windows) - RCE for Chrome, Firefox or Internet Explorer - RCE on Microsoft Office 2013-2019	n/a	n/a	dedicated RCS agent, separate for 32 and 64-bit OS: 1. remote installation using integrated exploit, after getting access/privileges manually 2. local installation, OS-level (CD/USB/Firewire DMA), needs privileges (like any other software) 3. local injection to hard drive connected to another computer 4. local injection using deep freeze mode (has some additional requirements, but possible)	↩	n/a	n/a	remote installation using CVE-2021-21166 and CVE-2021-30551 (Chrome), CVE-2021-33742 (Internet Explorer) - attack is performed on the browser, not full OS	local installation, separately for: 1. Internet Explorer, Firefox and basic system info 2. Skype (several different implementations, for various Skype versions)	dedicated FinSpy Target: 1. remote installation - possibly also using fake software updates (paid separately) 2. local installation from FinSpy U3-USB Dongle	1. local data exfiltration, via plugged-in USB device, support for Bitlocker / LUKS / VeraCrypt drive encryption 2. local injection of 3rd party exploits (possibly remotely exploitable), straight from USB device, without disconnecting the hard drive	- local data exfiltration, via plugged-in USB device - no drive encryption support - required logged in and unlocked Windows
3. Additional hardware implants	n/a	n/a	n/a	injecting hardware implant working below OS, used as an option - exploitation similar to BashBunny but smarter and through remote panel	↩	n/a	n/a	?	n/a	1. U3-enabled USB device (SanDisk Cruzer Micro U3) with additional software to simplify local infection - but without data exfiltration possibility. 2. Official FinFisher Remote Hacking Kit (version sold before 2013, then replaced with FinIntrusion Kit) contained also hardware PS/2 and USB keyloggers - both could be used separately from FinSpy Target.	n/a	
4. Post-install remote functionalities	standard package - access to: - Skype - Outlook - Telegram - Facebook - Gmail - device ID - browsing history - geolocation - raw files - passwords - keylogger - webcam - microphone recording - screenshots paid separately: - remote shell (Windows-only, 1.5M EUR) - Twitter - Viber - Signal - WeChat - Odnoklassniki - Vkontakte - Mail.ru	n/a	n/a	- Skype call and chat - Facebook chat and check-ins - Gmail and Outlook.com - Crypto currency transactions (e.g., BitCoins, LiteCoin, etc) - File capture - Camera snapshots - Key logging	↩	n/a	n/a	user's data available through browser, exfiltration is performed using WebSockets	1. remote access to: - basic computer/Windows information - list of local users - Firefox stored website passwords - Internet Explorer stored website passwords, browsing history and favourites 2. remote stealing Skype data, various attempts: - ptrace - hooking various versions of skype.exe - DirectSound - rootkit for Windows XP 3. later versions (2009+) - full audio/video recording	- File Access - Key-logging - Password Sniffing - Webcam Recording - Microphone Recordin - Timing based operations - Local Passwords (Windows, E-Mail clients, Messengers) - E-Mail Dumping (including SSL interception) - Chat Logging - Auto-removal - Live Update - IP change notification - Generic system information - Remote Command Shell	Only exploitation of locally injected 3rd party exploit(s).	GUI runs around 150 command line tools, that collect several information about the computer: - registry contents - filesystem contents - particular configuration details

LINUX												

PRODUCT KNOWN AS	- DevilsTongue - Sourgum	Pegasus	- Predator - SpearHead	- RCS - Da Vinci, Galileo - Scout, Soldier, Elite	RCS X	KRAIT	Hermit	SWR	- Bundestrojaner - MegaPanzer - MiniPanzer	- FinFisher - FinSpy - Wingbird	- Drive Badger - Funkcjonariusz	COFEE
DETAILS LAST UPDATED	**2022-06-19**	**2021-12-15**	**2022-06-18**	**2022-06-18**	**2022-06-18**	**2022-06-18**	**2022-06-18**	**2021-08-05**	**2021-08-30**	**2022-06-18**	**2022-06-18**	**2022-06-18**
Software-only installation and tracking method(s)	n/a	n/a	n/a	Dedicated RCS agent: 1. Has a lot of direct dependencies to X11, probably runs only on Linux with graphical environment. Versions supported due to pricing scheme document: Ubuntu, Debian, Mint. 2. Each platform has separate set of exfiltration modules (written as separate codebases). 3. Declared features: - Skype call and chat - Facebook chat and check-ins - Gmail and Outlook.com - Crypto currency transactions (e.g., BitCoins, LiteCoin, etc) - File capture - Camera snapshots - Key logging	↩	n/a	n/a	details unknown, but possibly Chrome on Linux can be supported	n/a	dedicated FinSpy Target, details unknown	1. local data exfiltration, via USB, support for Bitlocker / LUKS / VeraCrypt drive encryption 2. local injection of 3rd party exploits (possibly remotely exploitable), straight from USB, without disconnecting the hard drive	n/a
MAC OS												
Installation and tracking method(s)	not sure - depending on each source, supported or not	n/a	n/a	Dedicated 2 solutions: RCS agent + rootkit, and separate solution for local installation. Supported versions: from Snow Leopard to Yosemite. Features: - Skype call and chat - Facebook chat and check-ins - Gmail and Outlook.com - Crypto currency transactions (e.g., BitCoins, LiteCoin, etc) - File capture - Camera snapshots - Key logging	↩	n/a	n/a	?	n/a	dedicated FinSpy Target, details unknown	local data exfiltration only, via USB, support for APFS FileVault encryption, on T2-based models requires the device to already unlocked	n/a
MOBILE DEVICES												
General outcome and other comment(s)				in general, each mobile/desktop OS has completely different RCS implementation, with different abilities	↩			read user's data available through browser, exfiltrate using WebSockets			local data exfiltration only, once connected to Mobile Badger device - photos + most other in raw form, so it's a good idea to install and use apps like "export SMS to file" etc.	
ANDROID												
Installation and tracking method(s)	supported, there is a closed list of supported Android versions (4-9 as for 2020); documentation suggests that they may have problems with Android forks eg. Xiaomi MIUI - they support Samsung Galaxy S phones (and probably tablets), and agreed list of models/vendors for additional fee	remote: - magic sms/push, non-persistent infection, requiring re-infecting after each reboot - in non-root mode it can ask the user for permissions to access eg. photos, just like normal app supported Android versions: from 2.1, mainly Samsung Galaxy and Sony Xperia devices		supported, details unknown	↩			?	n/a	remote, using: - magic sms/push - Dirty Cow exploit local, by installing prepared app	local data exfiltration only, through MTP, PTP or Mass Storage (depending on Android version and security settings), requires already unlocked device	n/a
What information is available after installation	standard package - access to: - photos & screenshots - emails, sms - browsing history - contact details - calendar records - GPS location tracking - basic/advanced device info - call history - list directories - Google Drive - Dropbox - WhatsApp - FB Messenger - Skype - Telegram - network details - network change notifications - recording microphone and phone calls paid separately: - Twitter - Viber - Signal - WeChat - Odnoklassniki - Vkontakte - Mail.ru	- photos & screenshots - emails, sms - browsing history - contact details - calendar records - conversations from Skype, WhatsApp, Twitter, Facebook, Viber, KakaoTalk - GPS location tracking - device settings - network details - raw file retrieval - recording microphone and phone calls (Android-only)		- Skype call and chat - Facebook chat and check-ins - Gmail and Outlook.com - Crypto currency transactions (e.g., BitCoins, LiteCoin, etc) - File capture - Camera snapshots - Key logging	↩			?	n/a	access to: - photos & screenshots - emails, sms/mms - browsing history - contact details - calendar records - GPS location tracking - call history - BlackBerry Messenger - FB Messenger - InstaMessage - Line Messenger - Signal - Skype - Telegram - Threema - Viber - WhatsApp	- photos & screenshots - in MTP/MSC mode, everything that is remotely visible (access to raw files)	n/a
APPLE - iOS, iPadOS												
Installation and tracking method(s)	remote installation using either attack on Safari, or whole iOS (details not revealed)	remote, using: - magic sms/push - Trident exploit (CVE-2016-4655, CVE-2016-4656, CVE-2016-4657) - Kismet exploit (2020) - ForcedDentry (2021) previously known as Megalodon (2019) - existing jailbreak - emulation of clicking on important apps (eg. iMessage) non-persistent infection, requiring re-infecting after each reboot; supported iOS versions: from 4.x (iPhone 4)	supported iOS version at least 14.6	suported iOS versions: from 4.x to at least 8.1 (due to pricing scheme from 2014)	iOS is now supported up to 14.x		remote, using: - magic sms/push	remote installation using CVE-2021-1879	n/a	remote, using: - magic sms/push - Cydia Substrate's hooking functionality (iOS 11 and below, only jailbroken devices)	local data exfiltration only, through MTP, requires already unlocked device	n/a

PRODUCT KNOWN AS	- DevilsTongue - Sourgum	Pegasus	- Predator - SpearHead	- RCS - Da Vinci, Galileo - Scout, Soldier, Elite	RCS X	KRAIT	Hermit	SWR	- Bundestrojaner - MegaPanzer - MiniPanzer	- FinFisher - FinSpy - Wingbird	- Drive Badger - Funkcjonariusz	COFEE
DETAILS LAST UPDATED	**2022-06-19**	**2021-12-15**	**2022-06-18**	**2022-06-18**	**2022-06-18**	**2022-06-18**	**2022-06-18**	**2021-08-05**	**2021-08-30**	**2022-06-18**	**2022-06-18**	**2022-06-18**
What information is available after installation	standard package - access to: - photos & screenshots - emails, sms - browsing history - contact details - calendar records - GPS location tracking - basic/advanced device info - call history - raw file retrieval - Google Drive - Dropbox - WhatsApp - FB Messenger - Skype - Telegram - network details - network change notifications - recording microphone and phone calls (advertised but we doubt if really possible for this particular platform) paid separately: - Twitter - Viber - Signal - WeChat - Odnoklassniki - Vkontakte - Mail.ru	- photos & screenshots - emails, sms - browsing history - contact details - calendar records - converations from Skype, WhatsApp, Twitter, Facebook, Viber, KakaoTalk - GPS location tracking - device settings - network details - raw file retrieval		- Skype call and chat - Facebook chat and check-ins - Gmail and Outlook.com - Crypto currency transactions (e.g., BitCoins, LiteCoin, etc) - File capture - Camera snapshots - Key logging	↩		- Accessibility Event - Audio - Camera - File download - Notification Listener - WhatsApp - Account - Browser - Clipboard - File upload - Screen Capture - Address Book - Calendar - Device Info - Log - Telegram	?	n/a	access at least to: - emails, sms - BlackBerry Messenger - FB Messenger - InMessage - KakaoTalk - Signal - Skype - Telegram - Threema - Viber - WeChat - WhatsApp	everything that is remotely visible according to phone/tablet security settings (access to raw files)	n/a
WINDOWS MOBILE & PHONE												
Installation and tracking - Windows Mobile 5/6	n/a	?	n/a	dedicated RCS agent WM 5/6, the same that's later ported to WP8	↩	n/a	n/a	?	n/a	n/a	n/a	n/a
Installation and tracking - Windows Phone 7	n/a	?	n/a	it seems that support for WP7 was skipped	↩	n/a	n/a	?	n/a	n/a	n/a	n/a
Installation and tracking - Windows Phone 8 / 8.1	n/a	?	n/a	Dedicated RCS agent in "Modern Native" architecture, only for WP 8.0 and 8.1. Features: - Skype call and chat - Facebook chat and check-ins - Gmail and Outlook.com - Crypto currency transactions (e.g., BitCoins, LiteCoin, etc) - File capture - Camera snapshots - Key logging	↩	n/a	n/a	?	n/a	n/a	local data exfiltration only, through MTP, requires already unlocked device	n/a
Installation and tracking - Windows 10 Mobile	n/a	?	n/a	n/a	↩	n/a	n/a	?	n/a	n/a	local data exfiltration only, through MTP, requires already unlocked device	n/a
OTHER MOBILE DEVICES												
Installation and tracking - Symbian	n/a	supported Symbian versions: from 9.2	n/a	dedicated RCS agent; access to phone calls, microphone, SMS-es, calendar, address book, serials and configuration data, and raw filesystem	↩	n/a	n/a	?	n/a	n/a	supported Symbian versions: from 9.3, PTP-only, defective, local data exfiltration only, requires already unlocked device	n/a
Installation and tracking - BlackBerry (all versions)	n/a	BlackBerry supported versions: from 5.0 to 7.1 (Curve, Bold, Torch, Pearl), documentation didn't contain newer BlackBerry OS	n/a	dedicated RCS agent for J2ME (classic BB), partial support from 4.5, full from 5.0, installation requires a special C++ component that most probably has to be installed locally. Features: - Skype call and chat - Facebook chat and check-ins - Gmail and Outlook.com - Crypto currency transactions (e.g., BitCoins, LiteCoin, etc) - File capture - Camera snapshots - Key logging	↩	n/a	n/a	?	n/a	n/a	QNX only, local data exfiltration only, through MTP, requires already unlocked device	n/a
COSTS **(average, synthetized from many sources)**												
Annual cost per tracked user license (for first 10 users)	0	$65 000		€ 5,000				?	?	€ 35 100 for first 15 users	free	free
Annual cost per tracked user license (above first 10 users, up to next limit)	€ 100,000	$10 000		€ 4,000				?	?	€ 2340 per each tracked user, or € 1755 per each in 75-pack	free	free
Annual cost per operator	3 included + € 20 000 for each another	?		€ 5000 * 10 included				?	?	5 included + € 11 400 for each another	free	free
One time entry cost - excluding trainings	€ 16,850,000	€ 3,500,000		€ 530000 + € 240000 + € 230000				?	?	€ 2,700,000	only hardware cost	free (sponsored by Microsoft)
Trainings	?	€ 750,000		€ 55,000				?	?	€ 260,000	depends on training company, all documentation freely available	?
SOURCE CODE AVAILABILITY												
Source code status	closed source	decompiled samples only, mainly from Android agents		stolen, released half-officially on Github	closed source, however directly based on old code, which is available on Github	closed source	closed source	status unknown	early versions of client parts stolen, released half-officially on SF.net	closed source	open source	some of executed tools are open source, or freeware with available source code
Source code link	-	https://github.com/jonathandata1/pegasus_spyware		https://github.com/hackedteam/	-	-	-	-	https://sourceforge.net/projects/mega-panzer/ https://sourceforge.net/projects/mini-panzer/	-	https://github.com/drivebadger/	-
OTHER NOTES												
C&C infrastructure	?	Pegasus Anonymizing Transmission Network, up to 500 domains, DNS servers and others, to hide easy detection of traffic; on most platforms ability to self-destruct after 60 days of no connection, or after detecting non-target SIM card		Galileo RCS Anonymizer component (in fact, a modified "bbproxy" with added SSL support) was responsible for safeguarding the traffic. 3 licenses were included, each another costed € 50 000, anonymizers could be replaced for free within the license limit.				details unknown, probably all C&C infrastructure built separately per target	data exfiltration through SMTP with encrypted attachments, using pre-configured server name (without smtp-auth or TLS)	full details regarding 2008-2014 old FinSpy for PC here: https://wikileaks.org/spyfiles/files/0/310_ELAMAN-IT_INTRUSION_FINFISHER_INTRODUCTION_V02-08.pdf https://wikileaks.org/spyfiles/files/0/289_GAMMA-201110-FinSpy.pdf	No remote infrastructure is required, unless Drive Badger is weaponized using 3rd party exploit(s). As for local infrastructure: https://drivebadger.com/recommended-hardware.html https://drivebadger.com/mobile-recommended-hardware.html	No remote infrastructure is required.
Indicators of Compromise	https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/	https://github.com/AmnestyTech/investigations/tree/master/2021-07-18_nso https://arkadiyt.com/2021/07/25/scanning-your-iphone-for-nso-group-pegasus-malware/ https://sekurak.pl/czym-jest-oprogramowanie-szpiegowskie-pegasus-analiza-zagrozenia-oraz-metody-jego-wykrywania/		full code available on Github, several fragments of compiled code and particular techniques are very well detected by antivirus/security software (which makes them unusable for real attack)			https://www.lookout.com/blog/hermit-spyware-discovery			regarding 2018+ FinSpy mobile: https://securelist.com/new-finspy-ios-and-android-implants-revealed-itw/91685/		

PRODUCT KNOWN AS	- DevilsTongue - Sourgum	Pegasus	- Predator - SpearHead	- RCS - Da Vinci, Galileo - Scout, Soldier, Elite	RCS X	KRAIT	Hermit	SWR	- Bundestrojaner - MegaPanzer - MiniPanzer	- FinFisher - FinSpy - Wingbird	- Drive Badger - Funkcjonariusz	COFEE
DETAILS LAST UPDATED	**2022-06-19**	**2021-12-15**	**2022-06-18**	**2022-06-18**	**2022-06-18**	**2022-06-18**	**2022-06-18**	**2021-08-05**	**2021-08-30**	**2022-06-18**	**2022-06-18**	**2022-06-18**
Abuse prevention methods				Installations are limited to 50 infections.	Installations are limited to 25 or 50 infections.					Only 5 FinSpy Agent systems can login to the FinSpy Master and work with the data at the same time.	1. Intentionally there are no protections against operator abuse. 2. USB devices are protected against proving data exfiltration (to protect the operator, regardless of the situation).	No known protections against operator abuse.
More photos	https://sekurak.pl/devilstongue-czyli-lepszy-pegasus-od-izraelskiej-firmy-candiru/#comment-96837	https://niebezpiecznik.pl/post/jak-wyglada-rzadowy-trojan-pegasus-od-srodka/									https://drivebadger.com/history.html	https://niebezpiecznik.pl/post/cofee-z-tego-programu-korzysta-polska-policja/ https://www.kartook.com/applications/microsoft-cofee-application-list-on-second-thought/
Other materials	https://www.themarker.com/embeds/pdf_upload/2020/20200902-161742.pdf	https://wiadomosci.radiozet.pl/Polska/Polityka/Pegasus-w-Polsce.-CBA-kupilo-potezne-oprogramowanie-szpiegowskie https://s3.documentcloud.org/documents/4599753/NSO-Pegasus.pdf https://googleprojectzero.blogspot.com/2021/12/a-deep-dive-into-nso-zero-click.html		https://github.com/hackedteam/core-linux/tree/master/contrib					https://en.wikipedia.org/wiki/MiniPanzer_and_MegaPanzer		https://drivebadger.com/ https://funkcjonariusz.com/	

The above comparison was assembled by Tomasz Klim, https://github.com/tomaszklim/ - if you find it useful, consider donating my work: https://github.com/sponsors/tomaszklim