Top malwarové rodiny v České republice – srpen 2024			
Malwarová rodina	**Popis**	**Dopad v ČR**	**Dopad ve světě**
Androxgh0st	Androxgh0st je botnet zaměřený na platformy Windows, Mac a Linux. Pro infikování zařízení využívá několik zranitelností a zaměřuje se hlavně na PHPUnit, Laravel Framework a Apache Web Server. Krade citlivé informace, jako jsou informace o účtu Twilio, SMTP přihlašovací údaje, AWS klíče a podobně. Ke sbírání požadovaných informací používá soubory Laravel. Navíc má různé varianty, které vyhledávají různé informace.	7,28 %	5,34 %
Phorpiex	Phorpiex je botnet (známý také jako Trik), který je aktivní od roku 2010 a na svém vrcholu ovládal přes milion infikovaných počítačů. Šíří mimo jiné další malware prostřednictvím spamových kampaní a je také používán v kampaních zaměřených na sexuální vydírání.	4,60 %	4,52 %
BMANAGER	BMANAGER je modulární trojan, který pravděpodobně vytvořil hacker nazvaný Boolka. Boolka nejdříve využíval jen jednoduché skriptovací útoky, ale postupně začal používat sofistikované systémy pro šíření malwaru, včetně trojanu BMANAGER. Tento malware je součástí širší sady, která obsahuje různé komponenty určené ke krádeži dat a přihlašovacích údajů. BMANAGER se šíří především prostřednictvím SQL injection útoků na webové stránky, přičemž využívá zranitelnosti k zachycení uživatelských aktivit a ke krádeži dat.	4,02 %	0,80 %
FakeUpdates	FakeUpdates (nebo také SocGholish) je downloader napsaný v jazyce JavaScript. FakeUpdates šíří další malware, včetně GootLoader, Dridex, NetSupport, DoppelPaymer a AZORult.	4,02 %	8,22 %
Tofsee	Tofsee je Trickler, který je zaměřen na platformu Windows. Jedná se o víceúčelový nástroj, který lze použít k DDoS útokům, rozesílání spamu nebo třeba těžbě kryptoměn. Může také stahovat a spouštět další škodlivé soubory v napadených systémech.	3,45 %	0,92 %
FormBook	FormBook je škodlivý kód, který krade informace a zaměřuje se na operační systém Windows. Poprvé byl detekován v roce 2016 a je prodáván na nelegálních hackerských fórech. I když je jeho cena relativně nízká, má velmi dobré maskovací schopnosti. FormBook shromažďuje přihlašovací údaje z různých webových prohlížečů, vytváří snímky obrazovky, monitoruje a zaznamenává stisknuté klávesy a může stahovat a spouštět soubory na základě pokynů z C&C serveru.	2,68 %	2,84 %
Esfury	Esfury je červ, který umožňuje další útoky na napadený systém. Šíří se prostřednictvím vyměnitelných nebo síťových disků. Jakmile se Esfury dostane do počítače, připojí se ke vzdálené webové stránce a získává odtamtud příkazy. Esfury také změní výchozí stránku internetového prohlížeče a upraví nastavení systému. Navíc může změnit i řadu bezpečnostních nastavení a ukončit nebo zablokovat přístup k velkému počtu procesů. Esfury může přesměrovat vyhledávání na	2,30 %	0,85 %

	konkrétní reklamní webové stránky, jinak ovlivňovat prohlížení internetu nebo snížit rychlost sítě.		
TechJourney	TechnoJourney je adware, který se zaměřuje na systémy Mac. Je součástí adwarové rodiny AdLoad a zobrazuje vtíravé reklamy, které mohou vést na škodlivé webové stránky nebo spouštět stahování nechtěných souborů. Může také sledovat uživatelská data a aktivity uživatelů na internetu. Obvykle je distribuován prostřednictvím podvodných webových stránek nebo je připojen k jinému softwaru.	2,11 %	0,18 %
AZORult	AZORult je trojan, který shromažďuje a odesílá data z infikovaného systému. Jakmile je malware v systému nainstalován (obvykle je šířen nějakým exploit kitem, jako třeba RIG), může odesílat uložená hesla, lokální soubory, kryptopeněženky a informace o profilu počítače na vzdálený C&C server.	2,11 %	1,21 %
Authedmine	Authedmine je varianta nechvalně známého kryptomineru CoinHive. Používá se zejména k online těžbě kryptoměny Monero, nicméně před spuštěním těžebního skriptu vyžaduje výslovný souhlas uživatele.	2,11 %	0,08 %